THE INTERNATIONAL DEFENSE AND HOMELAND SECURITY SIMULATION WORKSHOP

SEPTEMBER 19-21 2012

VIENNA, AUSTRIA

DHSS
2012

EDITED BY

AGOSTINO BRUZZONE
WAYNE BUCK
FRANCESCO LONGO
JOHN A. SOKOLOWSKI
ROBERT SOTTILARE

PRINTED IN RENDE (CS), ITALY, SEPTEMBER 2012

ISBN 978-88-97999-00-3 (paperback)
ISBN 978-88-97999-08-9 (PDF)

ISBN 978-88-97999-00-3 (PAPERBACK)
ISBN 978-88-97999-08-9 (PDF)

THE INTERNATIONAL DEFENSE AND HOMELAND SECURITY SIMULATION WORKSHOP, DHSS 2012

SEPTEMBER 19-21 2012 - VIENNA, AUSTRIA

Organized by

DIME – University of Genoa

Liophant Simulation

Simulation Team

IMCS – International Mediterranean & Latin American Council of Simulation

DIMEG, University of Calabria

MSC-LES, Modeling & Simulation Center, Laboratory of Enterprise Solutions

Modeling and Simulation Center of Excellence (MSCOE)

Latvian Simulation Center – Riga Technical University

Logisim

LSIS – Laboratoire des Sciences de l'Information et des Systemes

MIMOS – Movimento Italiano Modellazione e Simulazione

MITIM Perugia Center – University of Perugia

Brasilian Simulation Center, LAMCE-COPPE-UFRJ

MITIM - McLeod Institute of Technology and Interoperable Modeling and Simulation – Genoa Center

M&SNet - McLeod Modeling and Simulation Network

Latvian Simulation Society

Ecole Superieure d'Ingenierie en Sciences Appliquees

Facultad de Ciencias Exactas. Ingegneria y Agrimensura

University of La Laguna

CIFASIS: CONICET-UNR-UPCAM

INSTICC - Institute for Systems and Technologies of Information, Control and Communication

National Russian Simulation Society

CEA - IFAC

Technically Co-Sponsored

IEEE – Central and South Italy Section Chapter

I3M 2012 Industrial Sponsors

CAL-TEK SRL

LIOTECH LTD

MAST SRL

I3M 2012 Media Partners

Inderscience Publishers – International Journal of Simulation and Process Modeling

Inderscience Publishers – International Journal of Critical Infrastructures

IGI Global – International Journal of Privacy and Health Information Management

Halldale Media Group: Military Simulation and Training Magazine

Halldale Media Group: The Journal for Healthcare Education, Simulation and Training

Euromerci

EDITORS

AGOSTINO BRUZZONE
MITIM-DIME, UNIVERSITY OF GENOA, ITALY
agostino@itim.unige.it

WAYNE BUCK
HQ SUPREME ALLIED COMMANDER TRANSFORMATION, USA
Wayne.Buck@act.nato.int

FRANCESCO LONGO
MSC-LES, MECHANICAL DEPARTMENT, UNIVERSITY OF CALABRIA, ITALY
f.longo@unical.it

JOHN A. SOKOLOWSKI
VIRGINIA MODELING, ANALYSIS AND SIMULATION CENTER, USA
JSokolow@odu.edu

ROBERT SOTTILARE
US ARMY, USA
Robert.Sottilare@us.army.mil

INTERNATIONAL MULTIDISCIPLINARY MODELING & SIMULATION MULTICONFERENCE, I3M 2012

GENERAL CO-CHAIRS

AGOSTINO BRUZZONE, *MITIM DIME, UNIVERSITY OF GENOA, ITALY*
YURI MERKURYEV, *RIGA TECHNICAL UNIVERSITY, LATVIA*

PROGRAM CHAIR

FRANCESCO LONGO, *MSC-LES, MECHANICAL DEPARTMENT, UNIVERSITY OF CALABRIA, ITALY*

THE INTERNATIONAL DEFENSE AND HOMELAND SECURITY SIMULATION WORKSHOP, DHSS 2012

GENERAL CO-CHAIRS

AGOSTINO BRUZZONE, *MITIM-DIME, UNIVERSITY OF GENOA, ITALY*
JOHN SOKOLOWSKI, *VIRGINIA MODELING, ANALYSIS AND SIMULATION CENTER, USA*

PROGRAM CHAIR

WAYNE BUCK, *HQ SUPREME ALLIED COMMANDER TRANSFORMATION, USA*
ROBERT SOTTILARE, *US ARMY, USA*

DHSS 2012 INTERNATIONAL PROGRAM COMMITTEE

Tayfur Altiok, Rutgers University, USA
Stuart Armstrong, QinetiQ, UK
Claudia Biasini, Swedish National Defense College, Sweden
Marco Biagini, University of Genoa, Italy
Linda Brent, The Asta Group, USA
Joy Bruce, Vastpark, USA
Agostino Bruzzone, University of Genoa, Italy
Wayne Buck, HQ Supreme Allied Commander Transformation, USA
Giovanni Cantice, Italian Army, Italy
Erdal Cayirci, University of Stavanger, Norway
Priscilla Elfrey, KSC-NASA, USA
Gene Fredriksen, Tyco International, USA
Claudia Frydman, LSIS, France
Johnny Garcia, Simis Inc., USA
Peggy Graviz, The Aegis, USA
Drew Hamilton, Auburn University, USA
John Illgen, Northrop Grumman, USA
Fred Lewis, NTSA, USA
Francesco Longo, University of Calabria, Italy
Marina Massei, Simulation Team, Italy
Francesco Mastrorosa, M&S COE, Italy
Roy Mitchell, Center for Operational Research and Analysis Defence R&D, Canada
Agatino Mursia, Selex Comm, Italy
Jackson P. Nelson , NTSA, USA
Gabriele Oliva, University Campus BioMedico of Rome, Italy
Tuncer Ören, University of Ottawa, Canada
Federica Pascucci, University of Roma 3, Italy
Paolo Proietti, Mimos, Italy
Elaine Raybourn, Sandia National Laboratories, USA
James Reynolds, GICSR, USA
Ronald Rolands, Rolands & Associated Corporation, USA
Rick Severinghaus, The Aegies, USA
Josh Singletary, National Health Information Sharing and Analysis Center, USA
John Sokolowski, VMASC, USA
Robert Sottilare, Army Research Laboratory, USA
Alberto Tremori, Simulation Team, Italy
Konstantinos Tsiakalos, MILTECH HELLAS SA, Greece
Michele Turi, University of Genoa, Italy
Walter F. Ullrich, HallDale Media Group, Germany
Bill Waite, The Aegis, USA
Richard Zaluski, CSCSS, UK
Aldo Zini, Cetena, Italy

TRACKS AND WORKSHOP CHAIRS

CONTEXT SIMULATION FOR DHS/HLS - "WHAT IS NEEDED TO SUPPORT FIRST REPONDERS"
CHAIR: JOHNNY GARCIA, SIMIS INC., USA.

PORTS AND LITTORAL PROTECTION
CHAIR: TAYFUR ALTIOK, RUTGERS UNIVERSITY, USA; FRANCESCO LONGO, UNIVERSITY OF CALABRIA, ITALY

SERIOUS GAMES: TOWARD EFFECTIVE TRAINING
CHAIRS: PAOLO PROIETTI, MIMOS, ITALY ; ELAINE RAYBOURN, SANDIA NATIONAL LABS/ADL , USA

URBAN AREA SECURITY
CHAIRS: ALBERTO TREMORI, SIMULATION TEAM, ITALY

CYBERSECURITY
CHAIRS: RICHARD ZALUSKI, CSCSS , USA; GENE FREDRIKSEN, TYCO INTERNATIONAL, USA

ADAPTIVE AND PREDICTIVE COMPUTER-BASED TUTORING
CHAIR: ROBERT SOTTILARE, ARMY RESEARCH LABORATORY, USA

NEXT GENERATION C4ISR MODELING & SIMULATION TECHNOLOGY: MIXED REALITY, CROWD SOURCING AND INTEROPERABLE C2-LVC ARCHITECTURES TO SUPPORT OPERATIONS, TRAINING, AND ANALYSIS
CHAIRS: MARCO BIAGINI, UNIVERSITY OF GENOA, ITALY; BRUCE JOY, VASTPARK, USA

SIMULATIONS AS TOOLS TO DEVELOP INTUITIVE CONTEXTUAL SENSITIVITY, RE-FRAMING, AND MENTAL AGILITY
CHAIRS: CLAUDIA BAISINI, SWEDISH NATIONAL DEFENCE COLLEGE, SWEDEN; ENRICO BOCCA, SIMULATION TEAM, ITALY

HOMELAND SECURITY: A CONTROL SYSTEM POINT OF VIEW
CHAIRS: GABRIELE OLIVA, COMPLEX SYSTEMS AND SECURITY LABORATORY UNIVERSITY CAMPUS BIOMEDICO OF ROME, ITALY; FEDERICA PASCUCCI, UNIVERSITY ROMA TRE, ITALY

General Co-Chairs' Message

Welcome To DHSS 2012!

Welcome to the International Defense and Homeland Security Simulation 2012 (DHSS 2012) Workshop Proceedings. There was significant excitement in the air this year as simulation experts from around the world assembled for our second DHSS workshop held in Vienna, Austria in September 2012. Selected articles cover different technical topics ranging from intelligent agents to mobile learning to serious games.

Simulation is presented as a tool of choice to train security methods within both military and civilian organizations. Within the DHSS 2012 articles Scientists share methods to enhance the performance of individuals and teams, reduce time and cost to develop simulation systems, and accelerate learning through intelligent agents. Engineers demonstrate practical tools to train, analyze, and deliver military and homeland security simulations. For reference a short description of the most important topic of the DHSS workshop tracks is described below:

Context Simulation for DHS/HLS provides a meta-analysis of what is needed to support first the training of first responders. Ports and Littoral Protection explores a wide variety of topics at the interface of port security, safety and port operations, with an emphasis on technical tools using mathematical modeling, risk analysis, and new algorithmic approaches to inspection of cargo, nuclear materials, vehicles entering ports, vessel movements in waterways and port operations.

Serious Games investigates the use of commercial games technologies, development of best practices, and barriers to further exploitation and ways these barriers might be overcome. Urban Area Security explores the unique challenges for training to maintain security in complex environments while CyberSecurity assesses methods for analyzing, recognizing, and remedying problems associated with information technology threats.

Adaptive and predictive computer-based tutoring focuses on tools and methods to support automated adaptation of instruction based on the learner's cognitive and affective states. Next generation C4ISR Modeling & Simulation technology examines simulation tools and methods including mixed reality, crowd sourcing, and interoperability between command and control and simulation architectures to support operations, training, and analysis.

Simulations as tools to develop intuitive contextual sensitivity, re-framing, and mental agility explore a sophisticated employment of simulation technology to enhance cognitive capabilities and stimulate brain plasticity. Finally, homeland security offers the possibility of representing results and identifying critical issues in complex homeland security environments.

Again, welcome and we hope you will find many useful topics in these proceedings and to meet your defense and homeland security training, analysis and operational needs and you will enjoy the wonderful framework of Vienna!

Agostino G. Bruzzone
Simulation Team MISS DIPTEM
University of Genoa, Italy

John Sokolowski
VMASC
Old Dominion University, USA

Wayne Buck
HQ Supreme Allied Commander
Transformation, USA

Robert A. Sottilare, Ph.D.
U.S. Army Research Laboratory, USA

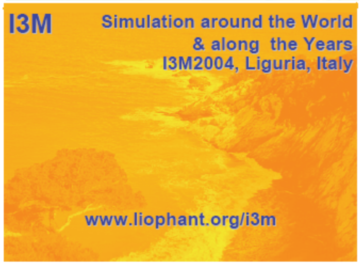
ACKNOWLEDGEMENTS

The DHSS 2012 International Program Committee (IPC) has selected the papers for the Conference among many submissions; therefore, based on this effort, a very successful event is expected. The DHSS 2012 IPC would like to thank all the authors as well as the reviewers for their invaluable work.
A special thank goes to all the organizations, institutions and societies that have supported and technically sponsored the event.

LOCAL ORGANIZATION COMMITTEE

AGOSTINO G. BRUZZONE, *MISS-DIPTEM, UNIVERSITY OF GENOA, ITALY*
ENRICO BOCCA, *SIMULATION TEAM, ITALY*
ALESSANDRO CHIURCO*, MSC-LES, UNIVERSITY OF CALABRIA, ITALY*
FRANCESCO LONGO, *MSC-LES, UNIVERSITY OF CALABRIA, ITALY*
FRANCESCA MADEO, *UNIVERSITY OF GENOA, ITALY*
MARINA MASSEI, *LIOPHANT SIMULATION, ITALY*
LETIZIA NICOLETTI, *CAL-TEK SRL*
ALBERTO TREMORI, *SIMULATION TEAM, ITALY*

This International Workshop is part of the I3M Multiconference: the Congress leading **Simulation around the World and Along the Years**



Index

UNDERWATER WARFARE SIMULATION IN DISTRIBUTED SYSTEM WITH DELTA3D

Won K. Hwam[a*], Yongho Chung[a], Young N. Na[b], Yongjin Kwon[a], Sang C. Park[a]

[a] Department of Industrial Engineering, Ajou University, South Korea
[b] Agency for Defense Development, Chinhaegu, ChangWon, Kyungnam, South Korea

[a*] lunacy@ajou.ac.kr

ABSTRACT

Forecasting performances of the weapon systems is very difficult to estimate as mathematical equations because there are many variables to consider. Modeling and simulation techniques have raised the optimal solution that can evaluate development and deployment of weapon systems. Simulation purposes are a decisive factor to design simulation systems, yet to develop a simulator for every single purpose is costly, un-swift, and inflexible. A distributed simulation system allows large-scaled simulations with economical input resources by linkages of existing simulators to the system, and it is also flexible and rapid to redesign the system for other purposes. This research implements underwater warfare simulation using Delta3D simulation game engine, originally designed for the military simulations, in a distributed system, and the simulation system interchanges environmental data due to underwater operations are mostly affected by environmental situations. This research adopts SEDRIS for environmental data and HLA/RTI for the distributed system.

Keywords: Delta 3D, HLA/RTI, SEDRIS, Underwater warfare

1. INTRODUCTION

Recently, military modeling and simulation (M&S) has remarkably grown in its importance and it is inevitable in the planning and operation of national defense strategies and war fighting efforts. The phenomenon is caused by the complexity of modern weapon systems which are highly increased by the development of the scientific technologies in comparison with weapons` history. The battle field of modern warfare is not the equal to the simple concept of the past, but it rather involves many complicated resources, such as network-centric warfare (NCW) concept (Lee and Wang, 2008). Therefore, modeling these high technologic weapon systems and battle field is not a simple question to gain the answer from mathematical equations. M&S is necessary to achieve cost-effectiveness weapon systems development, to examine the synergism of various weapon systems, and experiment environmental effects of the battle field to weapon systems, except for traditional purposes, such as training (Park Kwon Seong and Pyun, 2010).

Distributed simulation system helps to achieve various M&S objectives by integration of legacy simulators because existing simulation systems historically have been confined to single, isolated developed for single purpose. However, efforts to build new simulation system include large-scaled and complex modern warfare resources require tremendous time, cost, and human-power. Thus, distributed simulation system is in demand to obtain systems for various purposes with combination a multitude of individual simulations of existing simulators into larger simulations (ADSO, 2004). US Department of Defense (DoD) founded Defense Modeling and Simulation Office (DMSO) as an affiliated organization. The DMSO was renamed the Modeling and Simulation Coordination Office (M&SCO) in 2007. M&SCO has been leading DoD M&S standardization and empowering M&S capabilities to support the full spectrum of military activities and operations. M&SCO developed and released the IEEE 1516 High Level Architecture (HLA) standard which is distributed simulation architecture designed to facilitate interoperability and promote software reusability (M&SCO, 2012). Run-Time Infrastructure (RTI) is implementation of HLA and fulfillment of objectives of distributed simulation system.

In HLA/RTI systems and any military M&S applications, the environmental data are crucial in the depiction of the synthetic battle field situations, but the proprietary nature of various environmental data formats that reside in each simulation platform. It is a great impediment for the interoperability. The solution to this problem is the standard intermediate data format that permits the interchange of unified data between heterogeneous simulators. The Synthetic Environmental Data Representation and Interchange Specification (SEDRIS) provide a standard interchange mechanism for various environmental data. It increases the data reuse across diverse simulation platforms. SEDRIS addresses and represents all the aspects of synthetic environment, such as terrain, ocean, atmosphere, and space. SEDRIS supports a timely and authoritative representation of synthetic environment (Foley Mamaghani and Birkel, 1998). It bears the consecutive efforts that are dictated by the DoD M&S Master Plan (DMSO, 1995).

The representation of the environment to the synthetic battlefield is a critical factor in the simulation of naval warfare. This is multidimensional and it encompasses air, sea surface, sub-surface (underwater), land, space, and time. The survival and combat effectiveness of the naval force are considerably affected by the environmental factors of those dimensions. Command and control of naval warfare unifies ships, submarines, aircraft, and ground units. Thus, naval warfare system has a full range of environmental factors to represent the battle field. The underwater warfare is a part of naval warfare, and it inherits characteristics of a battle field of naval warfare. The general operation of underwater warfare is structured by using three forces, namely, submarines, surface ships, and air units. Figure 1 describes the concept of the future NCW-based anti-submarine operation system. It shows the integration of the combat units to accomplish a given mission (Mundy and Kelso, 1994).

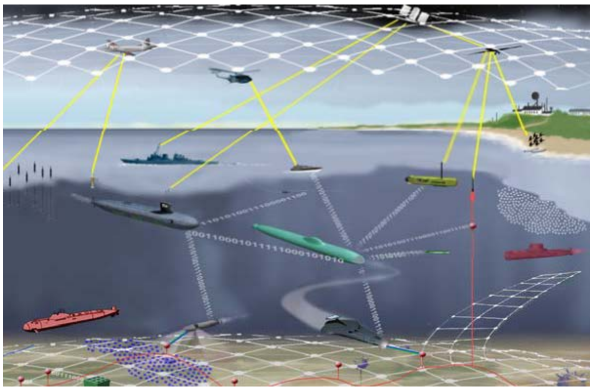


Figure 1: Anti-submarine Warfare Concept based on Network-Centric Warfare

Radar (an acronym for RAdio Detecting And Ranging) is an object-detection system that uses radio waves which do not work in underwater environment, as radio waves hardly penetrate through large volumes of water. Thus, the mean, instead of the radar, is sonar (an acronym for SOund Navigation And Ranging) and it detects objects that are under the sea by using sound propagation to identify objects, navigate, and communicate with other units under the sea. All submarines have sonar systems to navigate underwater, detect enemy, and so on. A submarine force has high capability to conceal itself, and it usually sails deep underwater. The submarine force can detect the surface ship force much easier compared to that of the surface ship force which detects the submarine force. It is precisely difficult to detect a submarine force to the surface ship force by itself, due to the environmental characteristics of underwater regarding sound propagation efficiency. Even if some surface ships have sonar systems for the anti-submarine operation, they load anti-submarine helicopter that has equipped dipping sonar to enhance their limited anti-submarine capability. The anti-submarine helicopter is one of the air force, and another is the anti-submarine plane. The dipping sonar hangs on the helicopter with a cable and it is dropped into underwater. The anti-submarine plane recognizes the electromagnetic waves of the submarines in the deep sea of flying area. The main assault weapon is the torpedo. It also has sonar system to navigate and detect the target (Brady and McCormick, 2008).

By considering of previous description of underwater warfare, the sonar is the most important system of the warfare. There are two types of sonars: passive sonar and active sonar. Passive sonar system is a sound-receiving system that uses hydrophones (underwater microphones) that receive, amplify, and process underwater sounds. Active sonar system emits pulses of sound waves that travel through the water, reflect off objects, and return to receiver. It can be the most effective means available for locating objects underwater. Active sonar system can be used to determine the range, distance and movement of an object. However, the performance of both types of sonar system depends on the environment and the equipped devices; receiver or emitter. To enhance the performance of the devices is limited, because the size of sonar has to be large enough to emit highly powered sound waves. Therefore, underwater operations are dependent on the environment in usual. The environment features affecting sonar operation are mostly sound speed, thermocline, and refraction of sound waves, and the three factors disturb sonar detection. For example, a ship equipped sonar system emits a sound wave, but the sound wave do not meet enemy submarine in thermocline area. Salinity and temperature are decisive environmental factors of those three features, yet the factors are various in the environment of underwater. Due to the variations in sound speed, the possibility to detect underwater objects using sonar is became different by the environmental factors. Consequently, it is now clear that the environment is the most important factor of the underwater warfare.

This paper explains constructing the underwater warfare simulation system, which needs environmental data to reflect environmental effects, based on the synthetic battlefield. This paper also provides an example implemented by Delta3D simulation game engine. The synthetic battlefield is constructed in SEDRIS, and it is supplied to the simulation from HLA/RTI based distributed system.

2. TECHNICAL APPROACH

The battlefield of the underwater warfare is able to model as a time-dependent three-dimensional grid space. It denotes an environment that is structured by time dimension, horizontal dimensions (i.e. latitude and longitude), and vertical dimensions (i.e. altitude and water depth). Figure 2 describes the structure, and it shows a three-dimensional grid space. The time-dependent denotes several of the structures along a lapse of the time dimension, and the time dimension identifies a data collection period. The structure generates cells that are defined by grid axes, and the each cell contains numerical values of the environmental properties.

In order to construct the synthetic battlefield for the underwater warfare, SEDRIS is adopted. SEDRIS has two core objectives. One is to represent environmental data, and the other is to interchange environmental data sets.

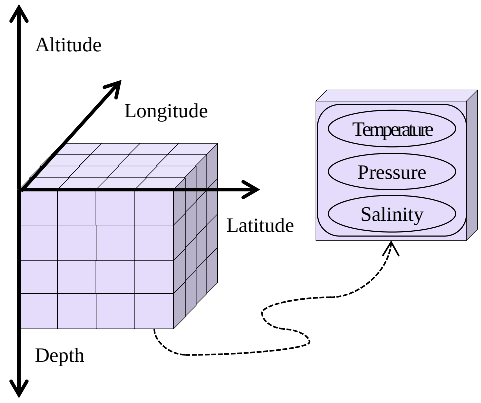
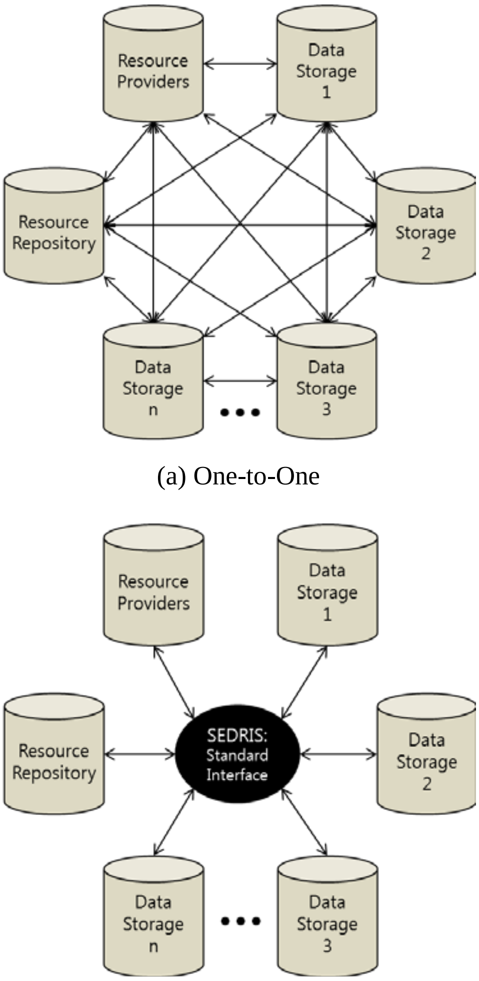


Figure 2: Environment Structure for Atmosphere/Ocean

In order to obtain the objectives, SEDRIS is composed of five components: Data Representation Model (DRM), Environmental Data Coding Specification (EDCS), Spatial Reference Model (SRM), SEDRIS Application Program Interface (API), and SEDRIS Transmittal Format (STF). DRM, EDCS, and SRM are core parts of SEDRIS, and STF is a product which is produced by combination of DRM, EDCS, and SRM. STF is also SEDRIS data file format which has information for describing environment, and this achieves the first objective of SEDRIS. SEDRIS API allows developers helping to access and generate STF with DRM, EDCS, and SRM. This makes SEDRIS achieve the second objective by data conversion between STF and others. There are SEDRIS API and STF to access and use SEDRIS core parts. SEDRIS API is constituted by DRM API, EDCS API, SRM API, and Transmittal Access API that is to make STF use all other APIs, and available on SEDRIS homepage. There are also many tools are free to open STF such as Focus, Model Viewer, Depth, Syntax checker, and Rule checker. SEDRIS can attain the interoperability in distributed simulation system as the standard format. Figure 3-(a) describes the point-to-point unique conversions between the data formats. This method requires converters for every data format, which needs 2 x (N-1)! (N: the number of data formats) converters. Therefore, this method can be very expensive and time consuming. Figure 3-(b) outlines the data interchange with SEDRIS as a standard interface with a common data model. This method can substantially reduce the conversion costs and related errors with the increased level of data reusability. As a standard interface, SEDRIS assumes a centralized intermediary between numerous environmental data formats (Welch, 1998).

The battlefield information is not a constant element, or rather changeable by scenarios that specify the place to take. It is also heavy and large data to manage in a battle simulator. Hence, it needs to be managed by an application, which is developed for environmental data only. HLA/RTI based distributed system is an appropriate approach to supply environmental data to the simulator.



(a) One-to-One

(b) Standard Interface

Figure 3: Data Interchange Methods

3. IMPLEMENTATION

Sonar is a technique that applies sound propagation to navigate, communicate with, and detect to other objects in underwater environment. A submarine has several sonar systems along with various purposes, for example, exploring the underwater ground, reconnaissance and detecting objects, identifying detected objects and tracing enemies, using passive and active sonar systems. The sonar operations are affected by variations in sound speed, particularly in the vertical plane. Several factors that affect performances of the sonar operations are also dependent upon the sound speed. Hence, modeling synthetic environment for underwater warfare simulation is devised to calculate the sound speed. There are two simple equations to calculate the speed of sound in seawater defined by Mackenzie (1981) and Coppens (1981).

The equation (1) for the speed of sound in seawater is given by Mackenzie.

Function Input:
T = Temperature in Degrees Celsius
S = Salinity in Parts per thousand
D = Depth in Meters

$$c(D,S,T) = 1448.96 + 4.591T - 5.304 \times 10^{-2}T^2 + 2.374 \times 10^{-4}T^3 + 1.340 (S-35) + 1.630 \times 10^{-2}D + 1.675 \times 10^{-7}D^2 - 1.025 \times 10^{-2}T(S - 35) - 7.139 \times 10^{-13}TD^3 \quad (1)$$

The equation (2 and 3) for the speed of sound in seawater is given by Coppens.

Function Input:
t = T/10 where T = Temperature in Degrees Celsius
S = Salinity in Parts per thousand
D = Depth in Kilometers

$$c(D,S,t) = c(0,S,t) + (16.23 + 0.253t)D + (0.213-0.1t)D^2 + [0.016 + 0.0002(S-35)](S - 35)tD \quad (2)$$

$$c(0,S,t) = 1449.05 + 45.7t - 5.21t^2 + 0.23t^3 + (1.333 - 0.126t + 0.009t^2)(S - 35) \quad (3)$$

Both equations are simple and old equations, but it is yet reliable and effective equations to derive the sound speed using environmental data. Along the requirements of two equations, temperature and salinity are the most important factors to know the sound speed. Therefore, the synthetic battlefield model for underwater warfare has to contain those two factors in each cell that are structured by three spatial-dimensions.

In HLA/RTI based distributed simulation system, the environment federate manages the environmental data, and it provides environmental data ranged by the request from the battle simulator. The battle simulator publishes spatial extent of the synthetic battlefield and subscribes the environmental data. The battle simulator calculates the sound speed using the subscribed environmental data, salinity and temperature. The calculated results are used to obtain the probabilities of the detection among the battle agents. The sonar operations are able to be modeled using the speed of sound propagation by sound transmission models, such as Range-dependent Acoustic Model (RAM) and Bellhop. The battle simulator includes these models to decide whether a submarine detects the enemy or not. Battle agents are allowed recognizing other agents by the battle simulator.

The underwater warfare simulation system, which is mentioned above, was implemented using Delta3D along a simple scenario. The scenario is an engagement between two submarines: A and B submarines. A submarine moves on patrol some area, and it keeps search to find enemies using its sonar system. B submarine goes from start point to the area that is guarded by A. A is assumed that it launches a torpedo to enemy submarine, if it had an enemy in sight. Even if B was navigating in the searchable perimeter of the sonar system of A, it is possible that A cannot realize the existence of B by the environmental effects.

Delta3D includes the openness of the source code, the flexible interface using various APIs, and the three-dimensional graphical simulation of combat entities (McDowell, 2006). For instance, its library contains basic infrastructure, and a unification layer, and in-between, includes graphics, geospatial data handling, character animation, GUI, audio, physics, networking, input handling, configuration system, unit testing, scripting, and additional miscellaneous features. Delta3D is sufficient tool to develop simulations for underwater warfare. The example was constructed using the C++ language. The pictures of Figure 4-7 are acquired from Delta3D visualization of the battle simulator during the underwater warfare simulation in HLA/RTI system.

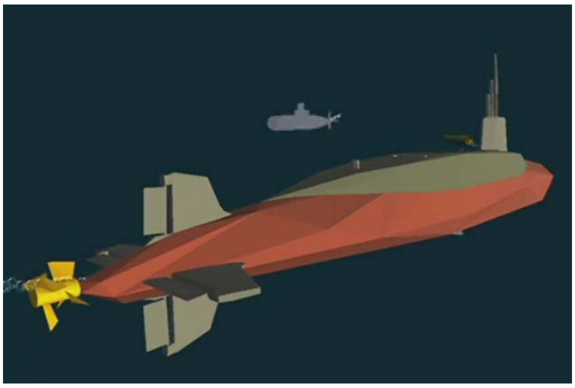


Figure 4: Submarine A Recognizes Submarine B

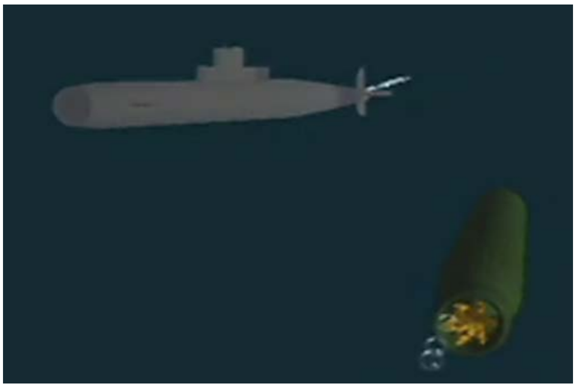


Figure 5: Submarine A Launches a Torpedo to B

Figure 6: The torpedo Traces Submarine B

Figure 7: Submarine B is Torpedoed by A

4. SUMMARY

Military M&S provides lots of benefits to achieve objectives of future warfare paradigm. M&S allows experiments of the new weapon system, before investing on the resources. So, we can find out the problems and modify in advance. It is an appropriate approach to develop a new weapon system effectively for unexpectable and changeable future battlefield. We are able to acquire new weapon system with minimized wastes of time, costs, and efforts by applying M&S. M&S brings the benefits, however, engineers must keep watch on the result of simulation because the result could contain unreliable or improper conclusions. It is caused by that decisive factors of the simulation had not reflected to fulfill the purposes of the simulation. In the underwater warfare, the underwater environment is the most important factor to simulate sonar operations. Therefore, modeling the synthetic battlefield of the underwater is one of necessaries to construct the technically reliable underwater warfare simulation system.

Environmental data usually include large amount of numerical data and the data are required to be reused. Therefore, handling the environmental data by the battle simulator is not an efficient approach to build simulation systems. There are demands of an application to manage the environmental data. Applying distributed simulation system allows engineers to link several different applications. Thus, engineers are able to build the underwater warfare simulation system that separates environmental data and a simulator. In the future goal, the simulation system will be constructed on the more precise sonar operation model.

ACKNOWLEDGMENTS

This work was supported by the Defense Acquisition Program Administration (DAPA) and the Agency for Defense Development (ADD) under the Contract No. UD100009DD (DAPA), UD110006MD & UD110071JD (ADD). This paper was also completed with Ajou University Research Fellowship of 2011. The authors wish to express sincere gratitude for the financial support.

REFERENCES

Australian Defense Simulation Office (ADSO), 2004. *Distributed simulation guide*. Canberra, Australia: Department of Defence.

Brady, P. H., McCormick, D., 2008. Undersea warfare division: A message from the naval undersea warfare center. *National defense industrial association* 24: 1-10.

Coppens, A.B., 1981. Simple equations for the speed of sound in Neptunian waters. *Journal of the Acoustical Society of America* 69(3): 862-863

DMSO, 1995. Modeling and simulation master plan. DoD 5000.59-P, USA.

Foley, P., Mamaghani, F., Birkel, P., 1998. *The SEDRIS Development Project*. SEDRIS Organization. Available from: http://www.sedris.org

Lee, K., Wang, J., 2008. Combined simulation for combat effectiveness analysis of land weapon systems. *Defense Science and Technology Plus* 63: 4-8.

Mackenzie, K.V., 1981. Nine-term equation for the sound speed in the oceans. *Journal of the Acoustical Society of America* 70(3): 807-812

McDowell, P., Darken, R., Sullivan, J., Johnson, E., 2006. Delta3D: A complete open source game and simulation engine for building military training systems. *The Society for Modeling and Simulation International* 3(3): 143-154.

Mundy, C. E. Jr., Kelso, F. B. II., 1994. Naval doctrine publication 1: Naval warfare. Department of the navy, Washington, D. C., USA.

M&SCO, 2012. *Description of M&SCO*. Available from: http://www.msco.mil/descMSCO.html

Park, S. C., Kwon, Y., Seong, K., Pyun, J. J., 2010. Simulation framework for small scale engagement. *Computers & Industrial Engineering* 59: 463-472.

Welch, M., 1998. *SEDRIS as an interchange medium*. SEDRIS Organization. Available from: http://www.sedris.org

BEYOND SERIOUS GAMES: TRANSMEDIA FOR MORE EFFECTIVE TRAINING & EDUCATION

Elaine M. Raybourn, Ph.D.
Sandia National Laboratories* and Advanced Distributed Learning Initiative
emraybo@sandia.gov, elaine.raybourn@adlnet.gov

ABSTRACT

Serious games present a relatively new approach to training and education for Defense and Homeland Security. Although serious games are often deployed as stand-alone solutions, they can also serve as entry points into training content that is delivered via different media. The present paper explores the application of transmedia storytelling used by entertainment, advertising, and the commercial game industries to sustain audience engagement with memorable experiences. Transmedia storytelling is the art and science of designing a consistent message that is delivered and reinforced across multiple media utilizing diverse entry points into a narrative to generate audience involvement with content. This approach is consistent with the goals of the Army Learning Model 2015 to deliver training and education to Soldiers across multiple media. Transmedia storytelling also provides a practical framework for developing media-rich training. In the present paper, we introduce the notion of transmedia storytelling, also known as transmedia or cross-media, as related to the use of serious games for training and education. We discuss why the human brain is wired for transmedia storytelling and demonstrate how the Simulation Experience Design Method can be used to create transmedia story worlds and serious games. Examples of how the U.S. Army has utilized transmedia for strategic communication and game-based training are provided. Finally, we conclude with strategies the reader can use today to incorporate transmedia storytelling elements such as Internet, TV, radio, print, social media, graphic novels, machinima, blogs, and alternate reality gaming into defense and homeland security serious game training.

Keywords: transmedia, cross-media, serious games, campaigns, storytelling

1. INTRODUCTION

Games have been used for a number of years in fields such as business and management science, economics, intercultural communication, and military science to expose both large and small audiences to complex dynamics. Military use of warfare board games dates back to 17th century Germany (McLeroy, 2008). Centuries later the United States Army War College was among the first to use networked, multiplayer simulations in the 1970s to refine mathematical models. The first use of a networked multiplayer computer game for training was by the United States Marine Corps. The United States Marines are among the earliest adopters of video game-based learning with the development of Marine Doom, a modified version of Id Software's Doom II, in 1995 (Riddell, 1997). Marine Doom was developed to allow four-person fire teams to train real-time teamwork and decision-making in an interactive virtual environment. Thus Marine Doom was the earliest modification of a commercial entertainment computer game for training and learning communication and coordination—not shooting or killing (Prensky, 2004). Since the late 1990's video games have been used by all branches of the Services for training and education, although most of this adoption has occurred in the last 8 years. These video games are often called "serious games."

Serious games can be defined as the use of interactive digital technologies for training and education in private, public, government, and military sectors (Raybourn, 2007). While there are many definitions for games, most identify some sort of conflict, rules, structure, goals, and uncertain outcomes as salient elements (Malone, 1980; Gredler, 1992; Crawford, 2003; Aldrich, 2004; Salen & Zimmerman, 2004; Bjork & Holopainen, 2004). For example, serious games can include games, role-play, and social-process, immersive simulations for exploring interpersonal development, adaptive thinking, combat tactics, emergency response, diplomacy, governance, health, education, management, logistics, and leadership.

Government use of serious games has grown steadily. The need for effective use of multiple media, immersive simulations, and gaming approaches for Homeland Security and Defense has never been greater. The United States military adopted serious game-based training for reasons that also appeal to many other organizations including reduced cost when compared to the cost for large simulators or live training, reaching digital natives who have grown up with technology, increased motivation to learn (Gee, 2003; Prensky, 2004), and the ability to leverage state-of-the-art technology. Twenty-first Century demands on training and education will extend the use of serious games and game technology beyond current approaches.

Proceedings of the International Defense and Homeland Security Simulation Workshop 2012
ISBN 978-88-97999-08-9; Bruzzone, Buck, Longo, Sokolowski and Sottilare Eds.

Serious game training and education must move beyond standalone solutions toward complete and enduring training experiences. This paper introduces the notion of Transmedia, an approach to emotionally connecting learners to content by involving them personally in training communicated across multiple media. We refer interchangeably to transmedia storytelling, transmedia campaigns, or simply transmedia as the same concept.

2. TRANSMEDIA STORYTELLING

Transmedia storytelling can be defined as crafting a narrative or consistent message (story) across multiple media. According to Henry Jenkins, "A transmedia story unfolds across multiple media platforms with each new text making a distinctive and valuable contribution to the whole" (Jenkins, 2006). It may be useful to consider transmedia projects as "campaigns." The term "campaign" as used in this paper will refer to a coordinated effort to link several media and training approaches to a single idea or theme. The use of transmedia campaigns for training and education is a cutting-edge approach that can help with retention, remediation, and knowledge reinforcement.

Utilizing transmedia campaign strategies, integral elements of a training narrative (e.g. warrior-diplomat ethos, first responder practices, etc.) get dispersed systematically across multiple delivery channels for the purpose of creating a unified and coordinated learner experience. Ideally, each medium makes its own unique contribution to the unfolding of the story. In this way, transmedia is a *system* that conveys a consistent communication message.

When crafting a training transmedia story, a designer can follow a typical framework for telling stories that involves taking the learner on an emotional journey from setting up the situation, introducing a conflict or challenge, allowing the tension to reach a high point or climax, and finally providing an opportunity for resolution (Raybourn & Silvers, 2011). This framework is often used in game design. Games provide players with experiences (Salen and Zimmerman, 2004). These experiences are often identified as being emotionally engaging (Fullerton et al., 2004) although as David Freeman (2004, p. 10) has stated, "you can't just suggest an emotion and assume the player will feel it." Creating true affect in games (as well as transmedia) requires satisfying learners' emotional needs or presenting different opportunities to explore emotions that learners may find appealing to try (Malone, 1982).

Similarly serious games for Homeland Security and Defense training can be interactive scenarios in which the learner is the protagonist of his or her own story. In particular Live Action Role Play (LARP) and multi-player games involve the learner from the first-person perspective. This first person buy-in is also key to transmedia storytelling. When learners are emotionally invested in the story, and in the case of training and education, see themselves as protagonists in their own training story, they not only remember it better, but they also continue to respond to new or repurposed content that is associated with familiar emotional triggers.

In the next section we introduce a new vision for Army training, The Army Learning Model (ALM) 2015 will require games and tools that not only interoperate, share data models, and tell their own unique stories but also deliver cohesive, cross-platform training that is memorable and increases retention. Transmedia provides a practical approach to designing cohesive learning instances that support a larger goal of motivating learners to train anytime, anywhere.

3. ARMY LEARNING MODEL 2015: WHY WE NEED TRANSMEDIA

Last year the United States Army formally identified a learning model to meet new requirements outlined in a Training and Doctrine (TRADOC) document, called the U.S. Army Learning Concept 2015 (Pamphlet 525-8-2). According to Pamphlet 525-8-2, page 3, "although the Army was an early adopter of distributed learning nearly 20 years ago, the program did not fully realize its intended goal of anytime, anywhere training." Army institutional training is still primarily comprised of instructor-led courses that are difficult to modify to meet individual learner's needs (Bickley et al., 2010). However, the Army has not abandoned its goal of anytime, anywhere training.

The ALM is a learning model that leverages personalized, self-paced instruction, and opportunities for peer interactions. The learning model can be best understood by applying Distributed Cognition Theory and the notion of "cognition in the wild." *Cognition in the wild* refers to human cognition as it naturally occurs and adapts in the everyday world—situated in culturally constituted human activity (Hutchinson, 1995). The ALM vision incorporates learner assessment while the learner naturally encounters content and experiences. "The future learning model must offer opportunities for Soldiers to provide input into the learning system throughout their career" as well as account for Soldiers' prior knowledge and experiences (Pamphlet 525-8-2, p. 6). Thus, the learning model represents training the way that people learn naturally—by formal and informal learning experiences in and out of the classroom and across learning platforms, simulations, games, social media, and intelligent tutoring systems.

In order to accomplish the ALM vision, blended, multi-media deployment and storytelling strategies incorporating serious games, immersive simulations, intelligent tutoring systems, virtual worlds, machinima (video or short films made with game technology), mobile learning, graphic novels, motion comics, film, radio, print, and social media will need to be leveraged effectively to motivate personalized, self-paced training and education. ALM presents a very ambitious vision that will require a paradigm shift in Defense and Homeland Security training. ALM training and education can leverage strategies common in cross-media, or transmedia storytelling used by entertainment, advertising, and the commercial games industries.

3.1 Army Learning Model Use Case

For example, recall the Army vision of a Soldier in 2015 who trains anywhere, anytime. In this use case a Soldier trains in the field, with different simulators, on different platforms, in the classroom, and with her peers (both co-located and distributed). The use of different media allows her to engage in the training from different entry points. Her training is comprised of interacting with one or more of the following technologies: intelligent computer-based tutoring, mobile performance aids, immersive virtual environments, serious games, augmented reality, machinima, graphic novels, peer-generated content, and social media. For instance, she may begin her language and culture training with an intelligent tutor and continue with a single-player scenario on cultural awareness that is delivered via a serious game. She engages in an alternate reality game on cultural awareness with her peers. Later she blogs about what she learned in her journal and shares this information with her team. The conversation about cultural awareness continues on Twitter. She reads about case studies via graphic novel or by watching videos. Her learning is self-paced, collaborative, adaptive, and/or mediated by instructors, virtual mentors, and embodied agents. She creates content, tracks her own learning, and monitors her progress. Most importantly, her training is delivered via a variety of media, making it more dynamic, accessible, and engrossing. Her training leverages best practices and advancements from the commercial game industry. Her training and education is delivered and reinforced via *transmedia*.

4. TRANSMEDIA FOR MORE EFFECTIVE TRAINING AND EDUCATION

According to Mark Long, Transmedia Producer and Co-Founder of Zombie, “We are in a transitional period where our relationship with media is shifting to multiple screens. Our audience is growing up in a digital world. The playing, reading patterns, and habits of young and old are changing as reading extends from the printed page to tablets and to a future of a myriad of diverse devices.” (Defense GameTech Keynote, March 2011) As noted by our example above, transmedia supports learning across a spectrum of devices by allowing the trainee to stay connected with training content throughout the day as she interacts with the devices and media to which she is accustomed. While it may not be possible to train all instances of a learning objective with a serious game, or any other technology for that matter, the training that is introduced can nearly seamlessly unfold while content is reinforced by other media. This is a big idea, representing a paradigm shift in the way we think about executing training and education.

To achieve a paradigm shift in training we will need to move beyond serious games as standalone digital learning instances. Current and future training and education realities necessitate a broader vision toward supporting serious game content with storytelling across multiple media to extend learning experiences beyond a single session. Even when learners are not playing a serious game, they can remain engaged with the training content especially if we apply transmedia.

Transmedia can augment serious game-based training because it blends story experiences to achieve buy-in from the trainee by allowing multiple entry points into the narrative, over several media. Transmedia does not imply design control over content—transmedia storytellers must allow learners to co-author the narrative by contributing their own experiences and interpretations (Giovagnoli, 2011). We allow for co-creation in transmedia because we seek to involve the learner cognitively and emotionally. That is to say, transmedia engages the brain and it behooves designers to understand how.

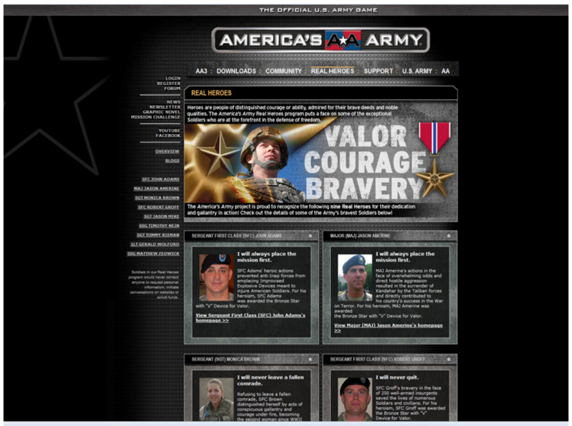
4.1 Transmedia, Emotions, and the Brain

Why does transmedia appeal to us on an emotional level? Why have stories been central to the human experience? Research indicates that it is primarily because the human brain is wired to pick up on messages crafted as stories because we feel real emotions when we connect with content or a character in a story. One potential explanation from LeDoux (1996) is that the brain uses two mnemonic systems to process information. The brain processes information both rationally and emotionally, although emotions about rational content are usually processed by the brain split seconds before rational or logical interventions by the cerebral cortex. The brain’s limbic system (thalamus, amygdala and hippocampus) reacts to information by interpreting sensory organ impulses sent by the thalamus to produce an emotion in the amygdala (LeDoux, 1997). LeDoux claims that perceptions (thalamus) and emotional responses (amygdala) always occur first—followed by judgments of like or dislike formed in the hippocampus. The limbic system generates emotional memories that make it easier for us to categorize and remember information. Put simply, LeDoux’s research indicates we best remember information presented in the form of a story. When done well, transmedia can evoke emotions that tap into sensations processed by the brain that may motivate a learner to have better retention of and connection to the content even when explored across several media.

5. ARMY GAME PROJECT: TRANSMEDIA FOR STRATEGIC COMMUNICATION

The first use of a concerted transmedia campaign was in 1976 to support George Lucas’ “Star Wars.” A publishing group was formed to produce and promote all products such as games, movies, toys, websites, cartoons, books, and comics associated with the film (Giovagnoli, 2011). The objective of a transmedia campaign is to create a fanbase that follows the transmedia experience across different media so as to not miss out on any part of the story.

Transmedia campaigns have also been used for Defense strategic communication in the America's Army franchise. The America's Army first person shooter game was conceived by Colonel Casey Wardynski of the US Army Economic and Manpower Analysis as a strategic communication tool to aid with recruitment, and especially to reach a fanbase of young people who were not likely to have had a family member that was in the US Army. Widely popular since 2002 with millions of fans worldwide, there have been over 26 publicly available versions released. The game is available by free download (http://www.americasarmy.com).



Soldiers in our Real Heroes program would never contact anyone to request personal information, initiate conversations on websites or solicit funds.

REAL HEROES

Heroes are people of distinguished courage or ability, admired for their brave deeds and noble qualities. The *America's Army* Real Heroes program puts a face on some of the exceptional Soldiers who are at the forefront in the defense of freedom.

The *America's Army* project is proud to recognize the following nine Real Heroes for their dedication and gallantry in action! Check out the details of some of the Army's bravest Soldiers below!

SERGEANT FIRST CLASS (SFC) JOHN ADAMS

I will always place the mission first.

SFC Adams' heroic actions prevented anti-Iraqi forces from emplacing Improvised Explosive Devices meant to injure American Soldiers. For his heroism, SFC Adams was awarded the Bronze Star with "V" Device for Valor.

View Sergeant First Class (SFC) John Adams's homepage >>

MAJOR (MAJ) JASON AMERINE

I will always place the mission first.

MAJ Amerine's actions in the face of overwhelming odds and direct hostile aggression resulted in the surrender of Kandahar by the Taliban forces and directly contributed to his country's success in the War on Terror. For his heroism, MAJ Amerine was awarded the Bronze Star with "V" Device for Valor.

View Major (MAJ) Jason Amerine's homepage >>

SERGEANT (SGT) MONICA BROWN

I will never leave a fallen comrade.

Refusing to leave a fallen comrade, SPC Brown distinguished herself by acts of conspicuous gallantry and courage under fire, becoming the second woman since WWII

SERGEANT FIRST CLASS (SFC) ROBERT GROFF

I will never quit.

SFC Groff's bravery in the face of 250 well-armed insurgents saved the lives of numerous Soldiers and civilians. For his heroism, SFC Groff was awarded the Bronze Star with "V" Device for Valor.

Figure 1. America's Army Real Heroes (courtesy of the Army Game Project).

A successful transmedia example of the America's Army franchise is the Real Heroes program (Raybourn & Silvers, 2011). Real Heroes was launched in 2006 to give the fanbase an opportunity to form emotional connections with real men and women of the U. S. Army who represent elite Soldiers serving their country with valor, courage, and bravery (see Figure 1). Real Heroes have been rendered in the America's Army game and sold as action figures. Players read their biographies and watch videos about how they received commendations from the U.S. Army. Some Real Heroes participate in the Virtual Recruiting Station where they interact with game players who then win bonus honor points for interacting with the Real Heroes (http://manual.americasarmy.com/index.php/Real_Heroes). The Real Heroes make public appearances at NASCAR events (sponsored by the U.S. Army) and other venues promoting the values and ethos of U.S. Army Soldiers.

The America's Army official website offers links to graphic novels (comics) that are available for viewing online or in print. The online versions are available on mobile devices and feature the use of motion comics. Figure 2 below illustrates how a narrative supporting Soldier operations can be communicated via a digital graphic novel (http://www.americasarmy.com). The use of dramatic colors, deliberately spaced panels on the page layout, and emotions on the faces of the characters are all crafted purposely to engage the audience and draw them into the story (McCloud, 1993).

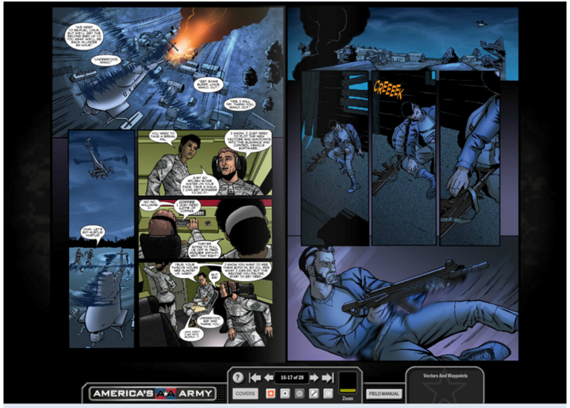


Figure 2. America's Army motion comic (courtesy of the Army Game Project).

The Army Game project also makes serious game applications. Although the game was initially meant for boosting recruitment, it was not long before America's Army Government Applications was formed to develop serious games for training and education. The first application of America's Army for training purposes was developed in 2003-2004 by Sandia National Labs and America's Army Government Applications (a.k.a. Virtual Heroes) for the U.S. Army Special Forces John F. Kennedy Special Warfare Center and School. The Special Forces cultural awareness and adaptive thinking multi-player game was called *America's Army Adaptive Thinking & Leadership* and was used to practice negotiation skills, cultural awareness, leadership, and adaptability (Raybourn et al., 2005). There have since been a number of follow-on Government applications used by the Secret Service, U.S. Army, and other combatant commands. Currently the Army Game Project is led by the U.S. Army Software Engineering Directorate located at the Redstone Arsenal near Huntsville, Alabama.

6. CREATING SERIOUS GAMES AND TRANSMEDIA CAMPAIGNS: SIMULATION EXPERIENCE DESIGN

Simulation Experience Design is a methodology and framework that can be used to create interactive stories, transmedia campaigns, and serious games. Simulation Experience Design treats game design as the creation of a *system of experiences* that exist within an emergent training context that the designer strives to reinforce throughout game play, as well as before, between, and after game play has concluded (Raybourn, 2007). The Simulation Experience Design methodology (Raybourn, 1999; 2004) is based on human-computer interaction (HCI) experience design principles that have been adapted for the design of serious games and transmedia storytelling. HCI experience design methods require that designers understand what makes a good experience first, and then translate the elements of the experience, as well as possible, into desired media without the technology dictating the form of the experience. Experience designers strive to create desired perceptions, cognition, and behavior among users, customers, learners, or the audience. For training and education purposes Simulation Experience Design is employed in the design of the entire transmedia or game system, from the design of scenarios, characters, roles, assessment interfaces, and associated media. This design method is based on the notion that the one's total experience is integral to the learning process.

There are at least four transmedia design principles that can be applied to Simulation Experience Design (see Figure 3): the development of Character (Interaction and Personas), Storytelling (Narrative and Scenarios), Worldbuilding (Place), and Audience Performance (Participation and Emergent Culture). We will use the example of the Real Heroes Program to illustrate each stage as well as provide insights for training.

In the interaction stage of the cycle emphasis is placed on identifying personas (Cooper, 1999) and roles. In this stage the transmedia designer would focus on understanding how the audience will interact with characters in the story. Focus is on developing an approachable character with which the learner can form an emotional bond. In the case of the Real Heroes Program the audience is the fanbase and the characters are the Real Soldiers who embody the values the transmedia campaign is attempting to convey. Their interaction in-game, through blogs, videos, photos, and Twitter feeds provide emotional ties to backstories and sidestories for the fanbase who is playing the America's Army game (Raybourn & Silvers, 2011). However in the case of training or education the learners are often both the audience and characters at any given time. Learners must see themselves as contributors to their own training story as first-persons, as well as have the opportunity to evaluate their performance from third-person point of views. For these reasons transmedia designers should allow for co-creation of narratives, characters, and interactions.

In the narrative stage designers co-create stories or scenarios that serve as the structure for learners to explore concepts. Here we ask the question, what is your training story? In the case of Real Heroes, their story is one of enduring Soldier ethos. The scenarios that play out are grounded in reality and open-ended—we are with them when they make public appearances, and we can talk to them in-game. In the case of transmedia training campaigns we ask the same question and this time build serious game scenarios and educational content that convey a believable, consistent message that learners can easily connect with. Learners can explore facets of unfolding episodes of a narrative through mobile devices, television, video, radio, Web, and print. We use a narrative framework of media elements that invite the learner into a world that goes beyond each individual medium to tell the story and also allows for co-creation.

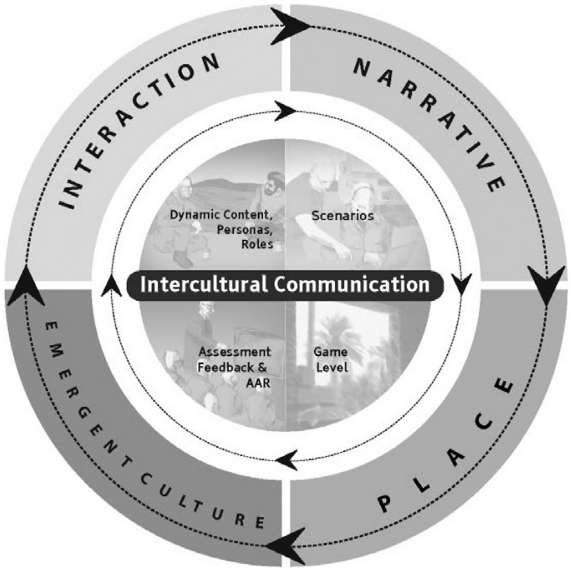

INTERACTION
NARRATIVE
PLACE
EMERGENT CULTURE
Dynamic Content, Personas, Roles
Scenarios
Intercultural Communication
Assessment Feedback & AAR
Game Level

Figure 3. Simulation Experience Design Framework (Raybourn, 2007).

In the third stage, place, designers consider the impact of the physical and virtual environments, or worlds, on narrative. In the case of the Real Heroes Program as well as training, place may be the serious game's immersive environment, an alternate reality game that occurs in both virtual and physical places, or the physical training environment in LARP. These environments allow the learner or audience to explore the world in the story interactively. There are a number of sidestories that might be developed as learners ask questions about place and seek to situate themselves in the story world.

Finally, the emergent culture stage presents an important component to successfully designed training which is the opportunity to reflect on experiences in the situated context (environment) in which the learning takes place (Lewin, 1951; Vincent & Shepherd, 1998). This collaborative reflection creates an emergent culture of audience participation and performance that acts as a foundation for the subsequent transmedia experiences (Raybourn, 2007). At this stage we can use social media for commentary on the training story as it evolves. Emergent culture is an opportunity to explore the broader training story in different ways to enrich the core experience.

7. ARMY GAMES FOR TRAINING: SERIOUS GAME TRAINING SUPPORT PACKAGES

Another example of a transmedia approach in use by the U.S. Army links the training story to a serious game. The Program Executive Office Simulation Training Readiness and Instrumentation (PEOSTRI) Games for Training Program produced 160 complete tasks from training support packages into graphic novels and machinima. Graphic novels similar to those utilized by the America's Army Game Project are currently in use by the U.S. Army to augment game-based collective training. The graphic novels set up the stand-alone scenarios in the serious game and provide interactive vignettes made from in-game machinima that demonstrate the right way to execute certain tasks. The interactive digital system includes instructor and student guides, tactical materials, After Action Review guides, and VBS2 game scenario files. The use of graphic novels to augment the serious game training allows learners to review tasks before and after gameplay. The graphic novels are reminiscent of the U.S. Army comic book series popular in the 1960's called the U.S. Army Preventive Maintenance Manual published by PS magazine. Since the content of the training support package (TSP) tasks must be accurate, this stylistic approach allows more tolerance for lengthy sections of text as it ties the TSP graphic novel to a format that is familiar. The comic book format focuses on episodic story elements (McCloud, 1993).

8. CONCLUSION

In summary, this paper described why transformational training experiences are necessary for Defense and Homeland Security, and how transmedia storytelling campaigns support the design requirements of the Army Learning Model. We discussed why transmedia storytelling is compelling and how these designs engage the human brain and emotions. We demonstrated how the Simulation Experience Design Framework (Raybourn, 2007) can be applied to both serious games and transmedia storytelling design. Finally, examples of how the U.S. Army utilizes transmedia for its strategic communication and serious game training were offered as examples of successful campaigns.

The author posits that 21st Century demands on training and education will require that we transform training practices. In particular there is a need to deliver training and education in Defense and Homeland Security across multiple media, providing the learner multiple entry points into the training. Transmedia was presented in this paper as a candidate to address this need. This paper addressed transmedia approaches inspired by the entertainment and commercial games industry that can be leveraged for application toward augmenting serious games for training and education. Future growth can be expected in the areas of serious games and transmedia for education and training as momentum gains and these approaches become more mainstream in Defense and Homeland Security sectors. New paradigms for 21st Century training and education require transformational strategies. Transmedia storytelling is a transformational technique used by the entertainment, advertising, and commercial game industries that is applicable to Defense and Homeland Security training and education.

Transmedia campaigns are the purposeful, coordinated, and strategic use of multiple media to relate a single, coherent story or narrative as it unfolds over time to engage new audience members or keep an audience engaged. Transmedia campaigns represent a unique opportunity to transform serious games and other tools for education and training from stand-alone learning instances to complete training experiences that transcend time and any one medium. This approach is not only consistent with the goals of the ALM 2015, but it can also provide a practical framework for developing media-rich training that presents cohesive and integrated content. Transmedia storytelling supports serious games to create transformational defense and homeland security training that goes far beyond stand alone solutions—toward more enduring and memorable training experiences.

ACKNOWLEDGEMENTS

The author thanks the U.S. Army Game Project, and Ms. Leslie Dubow of the U.S. Army Games for Training Program. *Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DEAC04-94AL85000.

REFERENCES

Aldrich, C. (2004). S*imulations and the future of learning*. San Francisco: Pfeiffer.

Bickley, W., Pleban, R., Diedrich, F. Sidman, J., Semmens, R., and Geyer, A. (2010). Army institutional training: Current status and future research, Army Research Institute Report 1921.

Bjork, S., & Holopainen, J. (2004). *Patterns in game design*. Boston: Charles River Media.

Cooper, A. (1999). *The inmates are running the asylum.* Indianapolis, IN: SAMS.

Crawford, C. (2003). *Chris Crawford on game design*. Indianapolis, IN: New Riders.

Freeman, D. (2004). *Creating emotions in games*. Indianapolis, IN: New Riders.

Fullerton, T., Swain, C., & Hoffman, S. (2004). *Game design workshop: Designing, prototyping and playtesting games*. San Francisco: CMP Books.

Gee, J. P. (2003). *What video games have to teach us about learning and literacy*. New York: Palgrave MacMillan.

Giovagnoli, M. (2011). *Transmedia storytelling: Imagery, shapes and techniques*. Pittsburgh, PA: ETC Press.

Gredler, M. (1992). *Designing and evaluating games and simulations: A Process Approach.* London: Kogan Page.

Hutchinson, E. (1995). *Cognition in the wild*. Cambridge, MA: The MIT Press.

Jenkins, H. (2006). *Convergence culture: Where old and new media collide.* New York: New York University Press.

LeDoux, J. E. (1996). *The emotional brain: the mysterious underpinnings of emotional life*. New York: Simon & Schuster.

Lewin, K. (1951). *Field theory in social science*. New York: Harper and Row.

Malone, T. (1980). What makes things fun to learn? Heuristics for designing instructional computer games. In Proceedings of the 3rd *ACM SIGSMALL symposium* and the first *SIGPC symposium on Small Systems* (pp. 162-169). New York: ACM Press.

Malone, T. (1982). Heuristics for designing enjoyable user interfaces: Lessons from computer games. In Proceedings of the 1982 *Conference on Human Factors in Computing Systems* (pp. 63-68). New York: ACM Press.

McCloud, S. (1993). *Understanding comics: the invisible art.* New York: Harper Perennial.

McLeroy, C. (2008). History of military gaming. *Soldiers Magazine*, 4-6.

Prensky, M. (2004). *Digital game-based learning*. New York: McGraw-Hill.

Raybourn, E. M. (1999). Designing from the interaction out: Using intercultural communication as a framework to design interactions in collaborative virtual communities. Presented at *ACM Group '99*, Phoenix, Arizona, November 14-17, 1999.

Raybourn, E. M. (2004). Designing intercultural agents for multicultural interactions. In Sabine Payr & Robert Trappl (Eds.), *Agent Culture: Human- Agent Interaction in a Multicultural World*, Lawrence Erlbaum, 267-285.

Raybourn, E. M., (2007). Applying simulation experience design methods to creating serious game-based adaptive training systems. *Interacting with Computers*, 19, Elsevier, 207-14.

Raybourn, E. M. (2011). Honing emotional intelligence with game-based crucible experiences. *International Journal of Game-Based Learning*, 1(1), IGI Global, 32-44.

Raybourn, E. M., Deagle, E., Mendini, K., & Heneghan, J. (2005). Adaptive thinking & leadership simulation game training for Special Forces Officers. I/ITSEC 2005 Proceedings of *Interservice/ Industry Training, Simulation and Education Conference*,November 28-December 1, Orlando, Florida, USA.

Raybourn, E. M. & Silvers, A. (2011). Transmedia Storytelling. Presentation delivered at ADL iFest, 2-4 August, Orlando, Florida. Retrieved from http://www.adlnet.gov/resources/transmedia-storytelling?type=presentation on July 15, 2012.

Riddell, R. (1997). Doom goes to war. *Wired*. Retrieved on July 15, 2012 from http://www.wired.com/wired/archive/5.04/ff_doom.html.

Salen, K., & Zimmerman, E. (2004). *Rules of play*. Cambridge, MA: MIT Press.

Vincent, A., & Shepherd, J. (1998). Experiences in teaching Middle East politics via Internet-based roleplay simulations. *Journal of Interactive Media in Education*, 98(11), 1-35. Retrieved from http://wwwjime.open.ac.uk/98/11 on July 15, 2012.

The U.S. Army Learning Concept for 2015. (2011). TRADOC Pamphlet 525-8-2.

AUTHOR BIOGRAPHY

Dr. Elaine Raybourn has a Ph.D. in Intercultural Communication with an emphasis in Human-Computer Interaction. She has led computer game research in multi-role experiential learning, social simulations, and designing training systems that stimulate intercultural communication competence, and adaptive thinking. She worked with PEOSTRI Games for Training on a transmedia augmentation to their serious game-based training. Elaine was on the advisory board for the Game Developers Conference (GDC) Serious Games Summit from 2004-2007 and is currently an Integrated Project Team (IPT) member of the I/ITSEC Training Subcommittee and Serious Games Showcase & Challenge as well as on editorial boards of the international journals *Interactive Technology and Smart Education*, *Journal of Game-based Learning*, and *Simulation & Gaming*. Elaine served as the 2011 Program Chair for the Defense GameTech Users' Conference. Elaine is a former ERCIM (European Consortium for Research in Informatics and Mathematics) fellow and a recipient of the Department of the Army Award for Patriotic Civilian Service, awarded to her by the U.S. Army Special Forces. Currently Elaine is on assignment from Sandia National Labs to the Advanced Distributed Learning Initiative, which is part of the Office of the Deputy Secretary of Defense (Readiness), where she leads research teams investigating adaptability, transmedia, and next generation learners' interactions with future learning technology such as personalized assistants for learning (PAL).

ADAPTIVE GAME-BASED TUTORING: MECHANISMS FOR REAL-TIME FEEDBACK AND ADAPTATION

Benjamin Goldberg[a], Keith W. Brawner [b], Heather K. Holden [c], Robert A. Sottilare [d]

[a,b,c,d]United States Army Research Laboratory—Human Research and Engineering Directorate—Simulation and Training Technology Center

[a]benjamin.s.goldberg@us.army.mil, [b]robert.sottilare@us.army.mil, [c]keith.w.brawner@us.army.mil, [d]heather.k.holden@us.army.mil

ABSTRACT

The advantages associated with game-based training platforms in the military domain are apparent. They enable Soldiers to practice the application of knowledge and skills in a safe simulated environment across multiple domains. However, simulation- and game-based training is limited in their ability to stand as instructional tools in the absence of live monitoring and instruction. Through the integration of computer-based tutoring technologies, game-based training has the potential to facilitate practice of executing tasks while having mechanisms to guide performance and facilitate instruction through embedded pedagogical functions. This poses many challenges that must be addressed. In this paper, the authors highlight desired functions and interactions between game-based platforms and computer-based tutoring architectures for support of real-time guidance and adaptation. Games provide unique environments for applying adaptations to specific scenario elements and for providing feedback on performance in real-time.

Keywords: adaptive tutoring, game-based training, real-time, feedback

1. INTRODUCTION

The role of simulation- and game-based training in the military domain is on the rise. They have proven to be an effective tool for enabling Soldiers to practice job relevant skills that are often too dangerous and too expensive to replicate in real world settings. This, in part, is due to continual advancements in computing technologies that enable the development of engaging and immersive interactive simulations that imitate tasks and conditions Soldiers face in theater. The target is to develop training systems that aid in the development of higher-order thinking skills that enable Soldiers to adapt decision-making tactics under variable missions and conditions (Wisher, Macpherson, Abramson, Thorton, and Dees, 2001). In today's combat environment, tasks are executed under a multitude of complex, stressful, and ambiguous settings where decisions must be quick and actions must be executed in a timely manner (Salas, Priest, Wilson, and Burke, 2006). To account for this, training aims at instilling the tenets linked to task execution and the values associated with decision making so as to facilitate an individual in making reasonable choices under difficult circumstances (Bratt 2009).

Videogame and scenario-based trainers are now being utilized to facilitate this need. Videogames are a practical solution because they provide engaging elements associated with their interaction and can be delivered across platforms commonly used in household and school environments. Furthermore, many games are traditionally developed with multiple players in mind. The use of multiple simultaneous players allows for the creation of team-based learning environments (Sottilare, Holden, Brawner, and Goldberg, 2011). However, traditional game design revolves around entertainment value rather than educational purpose. The core concept is that longer play times, or more frequent play, will result in higher profits. Subsequently, games are developed to keep people immersed and entertained, while consuming just enough content such that they do not abandon interaction. In the context of training, these experiential interactions provide realistic settings and conditions skills are executed within, but lack essential components of guidance and feedback inherent to learning. In this paper, the authors will highlight recent advancements in game-based training practices and identify components needed for the integration of adaptive functions. The pursuit is to develop reactive systems based on performance and state for the purpose of supporting individual differences associated with learning and retention.

1.1. Enhancing Game-Based Training

Relevant psychological theory would indicate that learning commonly occurs through experience, which can be replicated through real-life application or simulation (Kirschner, Sweller, and Clark, 2006; Kolb, Boyatzis, and Mainemelis, 2001). This edification represents experience in an environment where errors in performance can be linked to interactions taken, which stimulates deeper understanding of the effect decisions have on outcomes (i.e., cause and effect) (Mengel, 2012). An effective simulation-based training event replicates functional aspects of the real-world that influence action and drive training. However, simply applying and practicing skills in a simulated environment does not on its own promote expertise (Ericsson and Ward, 2007). Functions must be in place to tie game actions with training intent, thus linking performance with objective.

In recognition of this gap, serious games are designed to integrate pedagogical principles and strategies within videogame technologies to facilitate learning and skill development. The development of serious games, or games for the purpose of learning, is not a new idea (Apt, 1970), but is becoming increasingly more common practice (Raymer and Design, 2011). This genre uses an explicit approach where gameplay serves a purpose outside of entertainment by embedding educational functions into game events. Yet, while serious games are beginning to be used in a widespread context, and have decisions informed from sound instructional design methods, their effectiveness is limited to their developed intent and function.

In an attempt to enhance simulation-based training that can be facilitated outside of training environments, the pursuit of this research is to synthesize components of video games and intelligent tutors to deliver tailored training within game-based virtual environments. Specifically, the focus of this effort is to highlight the role adaptation and real-time feedback can play in making serious games a viable tool for both learning and practicing the application of knowledge and skills on the individual level. In the remainder of this paper we will discuss the mechanisms required for integrating personalized and adaptive capabilities in game-based training systems and the apparent restrictions for accomplishing this. Considerations serious game designers must take into account for supporting adaptive function will also be addressed.

2. APPLICATION OF ADAPTIVE TUTORING IN GAME-BASED TRAINING

In this section, we highlight on a conceptual level the functional requirements necessary for the authoring and integration of adaptive mechanisms in any game-based trainer. The notion is for the creation of a domain- and platform-agnostic framework to support the integration of personalized instructional strategies aimed at enhancing learning and motivation.

For an adaptive tutor to operate on a functional level within a game based environment, there are a number of faculties that must be in place for real-time support. This includes knowing what is being trained (domain model), knowing who is being trained (learner model), and knowing strategies for how to train most effectively based on the aforementioned information (pedagogical model). This knowledge is applied for customizing instructional strategies and tactics based on individual differences found to affect training outcomes. Artificial Intelligence (AI) tools and methods are applied to model these relationships and gauge a learner's current state of knowledge as they progress through a session (Kassim, Kazi, and Ranganath, 2004).

The traditional computer-based tutoring system (CBTS) loop consists of several phases (see Figure 1). The learner can be monitored on two dimensions: (1) affective/cognitive states via a suite of sensors and (2) assessment of learner actions within the instructional environment. These states, if present, are combined with an assessment of student actions as they relate to training objectives. Together, this picture generates the idea of whether an instructional intervention is required. If feedback is deemed appropriate, the system executes an authored strategy based on both the characteristics associated with the error in performance and the skills/abilities of the interacting user. Based on subsequent inputs, the system will adapt accordingly based on prescribed pedagogical principles.

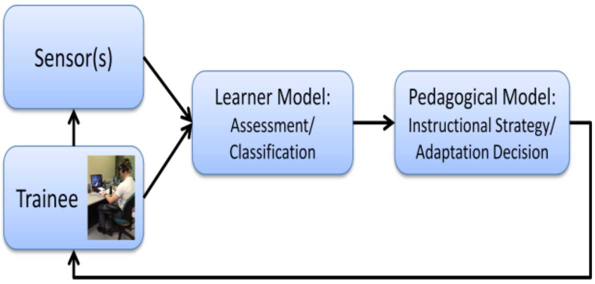


Figure 1: CBTS Loop

The strategies utilized in computer-based tutoring are based on personalized instructional and pedagogical heuristics applied within one-on-one expert tutoring. The benefit of this relationship is a tutor has the ability to guide and adapt instruction based on the strengths and weaknesses associated with a learner. In the context of simulation-based training this requires monitoring user interactions and using AI methods to assess performance and trigger adaptive interventions based on errors and diagnosed states as a result of training stimuli (Goldberg, Holden, Brawner, and Sottilare, 2011). In a Warfighter context, an effective computer-based tutor must have comprehensive knowledge of the operational context a scenario is designed around, have the capability to adapt to trainee fatigue and cognitive load, and to allow Soldiers to 'train as they fight' (Justice 2011). CBTSs must account for these requirements through robust modeling techniques.

2.1. Modeling for a Game-Based Environment

Enabling game-based training environments with adaptive resources is dependent upon the development of models that dictate interaction. This in turn requires assessment and prediction capabilities for both performance and state determinations as they relate to specific users and game engines. Performance metrics monitor progress towards objectives and errors present in execution, while state assessment gauges trainee reaction to training through the tracking of cognitive and affective variables linked to performance outcomes. In the context of game-based training, there are significant challenges associated with both of these functions. Multiple channels of data, derived from the game as well as the individual user, must be monitored and tracked to obtain the comprehensive knowledge needed for understanding learners' interactions within a game-based environment. One key requirement associated with this is the ability to assess both learner performance and state determinations in real-time.

Performance metrics are perhaps the easiest to monitor and include tracking progression towards targeted objectives, errors during execution, results on survey/test assessments during or after training, etc. Within traditional computer-based tutoring systems, performance metrics are used as the primary representation of a learners' current state of knowledge towards a particular domain (Woolf, 2009). This information is contained within a learner model and is used as a basis for adapting instruction as an individual's performance is compared to that of an expert (Kassim, et al., 2004). However, assessing performance requires explicit measures of how actions are related to objectives, which is often fuzzy in game-based environments. For example, what available data from a game designed in Virtual Battle Space 2 (VBS2) to train land navigation signifies a deficiency in calculating an azimuth from a protractor? The only available information is network traffic displaying entity state data, which in turn must be interpreted in relation to defined objectives that must be assessed. Determining a specific cause of performance deficiencies from game actions is an avenue of research that must be addressed.

To meet this need within a platform-agnostic framework, domain independent standards must be developed to author training objective metrics as they relate to system message traffic. However, when expanding adaptive tutoring to game-based training, monitoring the interactions between the game and the learner is more challenging than traditional static environments common to CBTS implementation. System concepts (i.e., inputs, processes, and outputs) vary between game platforms, and there is no unilateral or standardized way of interpreting learner interactions (Shute, Masduki, and Domnez, 2012). Yet, mapping and adapting system concepts to performance and state assessments across multiple games and platforms is achievable. A connection layer is required that translates game state information into user progress through the integration of assessments as they relate to event triggers present in the game world (Sottilare and Gilbert, 2011). This translation layer produces network traffic interpretable to a tutoring framework in terms of real-time game messaging associated with training objective performance. Having a standardized approach to this capacity would assist system developers in authoring message-based assessment models. This granular method makes identifying the root cause of an error achievable, which is essential for providing effective feedback or remediation in time of need.

In addition to real-time performance assessment, monitoring learner states (cognitive/affective) as they fluctuate during training interaction can provide valuable insight during game-based training. This information includes self-report instruments (surveys, interviews, etc.) and sensor technologies that monitor physiological and behavioral markers found to correlate with learning states (boredom, workload, confusion, frustration, etc.) (Carroll, Kokini, Champney, Fuchs, Sottialre, and Goldberg, 2011). Tracking states found to impact learning outcomes can be used to adapt content on the fly with the intention of keeping the user stimulated and motivated to continue interaction. The aim is to instill persistence in achieving objectives in an engaged manner that is conducive to effective knowledge transfer. In this context, research must be conducted to achieve the following functions:

1. Filtering and processing techniques of sensor data using standard computational and classification methods.
2. Functionality to combine sensor and self-report data, learner profile information, and events in the game world.
3. Development of windowed views (i.e., overall, previous, short-term, and long-term predictions) of learner cognition and affect.
4. Functionality to apply windowed learner state data to help interpret performance and apply context to state measures.

Consequently, game-based training platforms must also have mechanisms for acting on state and performance assessment results. This includes the ability to deliver feedback and adapt scenario elements as an individual progresses through task interactions. This is dependent on a platform-agnostic framework to allow the authoring of intervention strategies based on information pertaining to the objectives being monitored and characteristics unique to the individual user of the system. Feedback is provided to correct erroneous actions, promote reflection on concepts and actions taken, and mitigate misconceptions associated with training content (Mory, 2004). In-game adaptations should provide the ability to adjust difficulty levels based on individual performance, adjust the pace and flow of guidance and feedback, and deliver cues in the virtual environment that may act as a form of scenario specific feedback. In essence, these are the visible results produced by monitoring computer-based tutoring technologies. These mechanisms identified make up the desired functions of serious games for delivering tailored experiences, but current platforms lack many of the functions needed to support this approach.

A communication mechanism between the game world and the domain model is required to connect prescribed pedagogical interventions to associated game-specific actions. This mechanism should support both macro-adaptive and micro-adaptive functions, depending on the learner's knowledge, skills, and abilities within a particular domain. Macro-adaptive strategies can be applied to generate custom scenarios intended to balance flow (i.e., pace and challenge) based on learner attributes (Zook, Lee-Urban, Reidl, Holden, Sottilare, and Brawner, 2012). Macro-adaptation adjusts both game and tutor variables prior to interaction in an effort to personalize instruction. This can include varying the level of difficulty associated with a practice scenario and the how much guidance is provided when errors are present. Micro-adaptive strategies are based on real-time system interactions as they relate to defined objectives. Through an integrated CBTS, agents within the game world have knowledge about the learner and can react to requests from the tutor framework. An area receiving attention for this is Markov Decision Processes as they relate to tracking performance states within a training simulation. The notion is to research and develop techniques that can accurately gauge current, as well as predict performance states for the purpose of informing system adaptations. The CBTS can then apply modular, partially programmed agent behaviors that can be triggered by decisions within the pedagogical module. The desired functions highlighted in this section come with a wide array of challenges and questions that must be addressed among the CBTS research community.

3. LIMITATIONS AND FUTURE DIRECTION

The creation of personalized and adaptable serious games for training is of interest to the military and remains to be a challenging task. There are two primary reasons for this: increased developmental cost and associated research requirements. Game development traditionally has a special nature about it, as games and simulations are developed for specific clients under compressed schedules. Game developers frequently do not think to abide by the CBTS/Simulation Interoperability Standard (Stottler, Richards, and Spaulding, 2005), and focus upon the timely delivery of the product. To this effect, frequently each game has a different messaging structure associated with it. Even when a serious game obeys a standardized messaging structure, such as the Distributed Interaction System (DIS) protocol (IEEE, 1998), it is likely to have its own Application Programming Interface (API) for content injection. Depending upon the business structure of the creating company, these components can be closed, unavailable, or difficult to work with.

However, the developmental costs for embedding intelligent tutor capabilities in computer-based trainers are on the decline due to the availability of generalized architectural components that provide standardized practices for authoring tutor functions (Chipman, Olney, and Graesser 2005; Goldberg et al. 2011). This approach supports the development of such systems in significantly less time and with significantly less effort. The generalized approach also supports the authoring and integration of adaptive tutoring functions in already developed games utilized as practice tools following traditional classroom instruction. In a Department of Defense context, there is likely to already be an existing serious game, simulation, or practice environment for the skills taught in a classroom environment. These can be leveraged into existing domain-independent CBTS infrastructures to provide the traditional one sigma of learning gain (Verdu, Regueras, Verdu, Castro, and Perez, 2008) associated with computer-based tutoring, at a relatively low developmental cost. For these reasons, it is attractive to leverage the advantages gained from serious games and game-based environments into the instructional domain of computer-based tutoring.

As mentioned earlier, serious games typically have an Application Programming Interface (API), through which domain content and instructional strategy decision inputs can be captured. This enables interaction between tutoring agents and game-based applications (see Figure 2). Through this communication flow, a CBTS can inform actions to be executed in the game world. The challenge associated with this is applying context to game interaction. For a tutoring agent to effectively act on the game events, the agent must be able to observe the game world and determine the effect behaviors have on game objectives. It is expected that the use of these two technologies will increase, provided that the underlying research on instructional strategies continues.

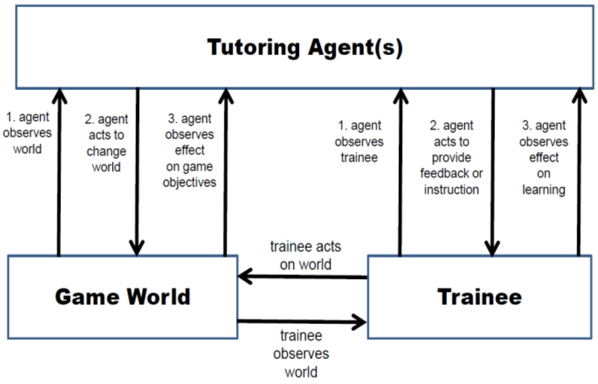

Tutoring Agent(s)
1. agent observes world
2. agent acts to change world
3. agent observes effect on game objectives
1. agent observes trainee
2. agent acts to provide feedback or instruction
3. agent observes effect on learning
trainee acts on world
Game World
Trainee
trainee observes world

Figure 2: Interaction in Game-Based Tutoring (from Sottilare, 2012)

In addition to developmental limitations, there is also a lack of research on how to effectively adapt instruction and provide feedback within a game environment. This requires two research themes. Identifying techniques for linking scenario specific actions in game environments to defined training objectives and concepts, and identifying adaptation and intervention techniques that do not hamper the benefits associated with game-based training. In order to adapt effectively, empirical research must be conducted to examine feedback and adaptation approaches specifically for virtual game-based environments. Open questions in this area include the comparison of within-game feedback, out-of-game feedback, and within-game character feedback. In addition to reductions in CBTS-game development cost, intelligent tutor architectures also support the design of comparative and ablated studies on adaptation methodologies to test the effectiveness of various instructional strategies.

Overall, the primary hurdle associated with this endeavor is linking game actions and states to specific training objectives the game is designed to instill. From this stance, two efforts currently dominate the minds of the authors in order to address the multi-interface, multi-environment, multi-tutor problem. The first is the development of game interlingua, a common translated language for CBTSs and games. This standardizes communication protocols between game engines and tutoring architectures, eleminating the need for solutions dependent to game messaging structures. The second effort is the development of a simulation connection layer which can translate messages coming out of multiple game enviroments. This is intended to help alleviate the previously mentioned problem. Both of these solutions may require slight modifications to existing game interface layers, but this requires only one instance for the tutoring system in question. This type of solution, coupled with the development of a domain-independent authoring tool for relaying real-time performance assessments (ECS, 2012), may help to transition game and CBTS research to the schoolhouse.

4. CONCLUSION

The authors would urge Serious Game developers to consider the impacts adaptive tutor functions can have upon their products. They have the ability to leverage components and research at a very low cost, provided that they are willing to encode training focused guidance and adaptation in a meaningful way. This aids the designer in two ways: the knowledge requirement for instantiating instructional strategies is significantly decreased, and the ability to claim educational impact significantly increases.

REFERENCES

Apt, C., 1970. *Serious Games*. New York: The Viking Press.

Bratt, E. O., 2009. Intelligent Tutoring for Ill-Defined Domains in Military Simulation-Based Training. *International Journal of Artificial Intelligence in Education*, 19, 337-356.

Carroll, M., Kokini, C., Champney, R., Fuchs, S., Sottilare, R., Goldberg, B., 2011. Modeling trainee affective and cognitive state using low cost sensors. *Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC*. November 28 – December 1, Orlando (Florida, USA).

Chipman, P., Olney, A., Graesser, A. C., 2005. The AutoTutor 3 architecture: A software architecture for an expandable, high-availability ITS. In: Cordeiro, J., Pedrosa, V., Encarnacao, B., Filipe, J,. eds. *Proceedings of WEBIST 2005: First International Conference on Web Information Systems and Technologies*. Portugal: INSTICC Press, 466-473.

Engineering and Computer Simulations, Inc., 2011, *Simulations for Integrated Learning Environments (SIMILE).* Engineering and Computer Simulations, Orlando. Available from: http://www.ecsorl.com/products/simile [accessed 09 July 2012]

Ericsson, K. A., Ward, P., 2007. Capturing the Naturally Occurring Superior Performance of Experts in the Laboratory: Toward a Science of Expert and Exceptional Performance. *Current Directions in Psychological Science,* 16(6), 346-350.

Goldberg, B., Holden, H. K., Brawner, K. W., Sottilare, R. A., 2011. Enhancing Performance through Pedagogy and Feedback: Domain Considerations for Intelligent Tutoring Systems. *Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC),* November 28 – December 1, Orlando (Florida, USA).

Institute of Electrical and Electronics Engineers (IEEE). (1998). IEEE 1278.1A-1998, Standard for Distributed Interactive Simulation - Application Protocols Errata.

Kassim, A. A., Kazi, S. A., Ranganath, S., 2004. A Web-based intelligent learning environment for digital systems. *International Journal of Engineering Education,* 20(1), 13-23.

Kirschner, P. A., Sweller, J., Clark, R. E., 2006. Why Minimal Guidance During Instruction Does Not Work: An Analysis of the Failure of Constructivist, Discovery, Problem-Based, Experiential, and Inquiry-Based Teaching. *Educational Psychologist,* 41(2), 75-86.

Kolb, D. A., Boyatzis, R. E., Mainemelis, C., 2001. Experiential Learning Theory: Previous Research and New Directions. In: Sternberg, R.J., Zhang, L. eds. *Perspectives on thinking, learning, and cognitive styles: The educational psychology series*. Mahwah, NJ: Erlbaum, 227-247.

Mengel, F., 2012. Learning across games. *Games and Economic Behavior,* 74, 601-619.

Mory, E.H., 2004. Feedback Research Revisited, In: Jonassen, D.H., ed. *Handbook of Research for Educational Communications and Technology.* New York: Macmillan Library Reference USA, 919-956.

Raymer, R., Design, E. L., 2011. Gamification-Using Game Mechanics to Enhance E-Learning. *Elearn Magazine,* 9(3).

Salas, E., Priest, H. A., Wilson, K. A., Burke, C. S., 2006. Scenario-based training: Improving military mission performance and adaptability. In: A. B. Adler, A.B., Castro, C.A., Britt, T.W., eds. *The psychology of serving in peace and combat operational stres.* Westport, CT: Greenwood Publishing Group, Inc., Vol. 2.

Shute, V., Masduki, I., Donmez., O., 2010. Conceptual Framework for Modeling, Assessing, and Supporting Competencies within Game Environments. *Technology, Instructional, Cognition and Learning,* 8, 137-161.

Sottilare, R.A., Gilbert, S., 2011. Considerations for Adaptive Tutoring within Serious Games: Authoring Cognitive Models and Game Interfaces. *Proceedings of the International Conference on Artificial Intelligence in Education (AIED) 2011*, June 28 – July 1, Auckland, New Zealand.

Sottilare, R. A., Holden, H. K., Brawner, K. W., Goldberg, B. S., 2011. Challenges and Emerging Concepts in the Development of Adaptive, Computer-based Tutoring Systems for Team Training. *Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)*. November 28 - December 1, Orlando (Florida, USA).

Sottilare, R., 2012. Enhancing the Power of Game-based Training with Adaptive Tutors Tutorial. *Presented at Defense GameTech*, Orlando, Florida. March 2012.

Stottler, R. H., Richards, R., Spaulding, B. 2005. Use cases, requirements and a prototype standard for an Intelligent Tutoring System (ITS)/Simulation Interoperability Standard (I/SIS). *Proceedings of the SISO 2005 Spring Simulation Interoperability Workshop*, April 3 – 8, San Diego, CA.

Verdu, E., Regueras, L. M., Verdu, M. J., Castro, J. P. D., Perez, M. A., 2008. Is Adaptive Learning Effective? A Review of the Research. *Wseas Advances on Applied Computer and Applied Computational Science*, 710-715.

Wisher, R. A., Macpherson, D. H., Abramson, L. J., Thorton, D. M., Dees, J. J., 2001. The Virtual Sand Table: Intelligent Tutoring for Field Artillery Training (ARI Research Report 1768). Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Science, DTIC No. AD-A388 158.

Woolf, B.P., 2009. *Building Intelligent Interactive Tutors: Student-Centered Strategies for Revolutionizing E-Learning*. Burlington, MA: Elsevier.

AUTHORS' BIOGRAPHY

Benjamin Goldberg is a member of the Learning in Intelligent Tutoring Environments (LITE) Lab at the U.S. Army Research Laboratory's (ARL) Simulation and Training Technology Center (STTC) in Orlando, FL. He has been conducting research in the Modeling and Simulation community for the past four years with a focus on adaptive learning and how to leverage Artificial Intelligence tools and methods for adaptive computer-based instruction. Currently, he is the LITE Lab's lead scientist on instructional strategy research within adaptive training environments. Mr. Goldberg is a Ph.D. student at the University of Central Florida and holds an M.S. in Modeling & Simulation. Prior to employment with ARL, he held a Graduate Research Assistant position for two years in the Applied Cognition and Training in Immersive Virtual Environments (ACTIVE) Lab at the Institute for Simulation and Training.

Keith Brawner is a researcher for the Learning in Intelligent Tutoring Environments (LITE) Lab within the U. S. Army Research Laboratory's Human Research & Engineering Directorate (ARL-HRED). He has 6 years of experience within U.S. Army and Navy acquisition, development, and research agencies. He holds an M.S.in Computer Engineering with a focus on Intelligent Systems and Machine Learning from the University of Central Florida, and is a Ph.D. candidate for doctoral degree in the same field. Current focus of research is in machine learning, adaptive training, affective computing, datastream mining, and semi/fully automated user tools for adaptive training content.

Heather K. Holden, Ph.D. is a researcher in the Learning in Intelligent Tutoring Environments (LITE) Lab within the U.S. Army Research Laboratory – Human Research and Engineering Directorate (ARL-HRED). The focus of her research is in AI and CBTS application to education and training; technology acceptance and Human-Computer Interaction. Dr. Holden's doctoral research evaluated the relationship between teachers' technology acceptance and usage behaviors to better understand the perceived usability and utilization of job-related technologies. Her work has been published in the Journal of Research on Technology in Education, the International Journal of Mobile Learning and Organization, the Interactive Technology and Smart Education Journal, and several conference proceedings. Her PhD and MS were earned in Information Systems from University of Maryland, Baltimore County and a BS in Computer Science from the University of Maryland, Eastern Shore.

Robert A. Sottilare, Ph.D. is the Associate Director for Science & Technology within the U.S. Army Research Laboratory - Human Research and Engineering Directorate (ARL-HRED) and directs research within the Learning in Intelligent Tutoring Environments (LITE) Laboratory at ARL's SFC Paul Ray Smith Simulation & Training Technology Center (STTC). He has 28 years of experience as both a U.S. Army and Navy training and simulation researcher, engineer and program manager. He leads the international program at STTC and chairs training technology panels within The Technical Cooperation Program (TTCP) and NATO. Dr. Sottilare holds a patent for a high-resolution, head-mounted projection display and his recent publications have appeared in the Educational Technology Journal, the Journal for Defense Modeling and Simulation and the proceedings of the Intelligent Tutoring Systems Conference 2010. He is a graduate of the Advanced Program Managers Course at the Defense Systems Management College, and his doctorate in modeling & simulation with a focus in intelligent systems is from the University of Central Florida. In January 2012, Dr. Sottilare was honored as the inaugural recipient of the U.S. Army Research Development & Engineering Command's (RDECOM's) Modeling & Simulation Lifetime Achievement Award. The focus of his current research is on the application of artificial intelligence tools and methods to adaptive training environments.

CONSIDERATIONS IN THE DEVELOPMENT OF AN ONTOLOGY FOR A GENERALIZED INTELLIGENT FRAMEWORK FOR TUTORING

Robert A. Sottilare, Ph.D. [(a)]

[(a)] U.S. Army Research Laboratory – Human Research & Engineering Directorate
Learning in Intelligent Tutoring Environments (LITE) Laboratory

[(a)] robert.sottilare@us.army.mil

ABSTRACT

Tutoring research has been ongoing on since the 1960s and workable computer-based tutoring systems (CBTS) have been around since the early 1980s. Expectations are on the rise for CBTS to be available to the masses in much the same way that human tutoring is available from a variety of sources today. A limiting factor in the widespread use of CBTS is the cost to: author tutoring systems; author/deliver domain-specific instructional content; and assess the effectiveness of CBTS tools and methods. A structural framework to represent knowledge within the CBTS domain would enhance reuse and streamline processes making them easier to author on production line scale, and opening the entry point for CBTS to non-computer scientists. This paper considers the benefits and challenges in developing an ontology for a Generalized Intelligent Framework for Tutors (GIFT) to support the development of authoring, instructional and assessment standards and tools for CBTS.

Keywords: adaptive computer-based tutoring, ontology, frameworks, authoring, instruction, assessment

1. INTRODUCTION

In 2004, Loftin, Mastaglio and Kenny declared that "while one-to-one human tutoring is still superior to [computer-based tutoring systems] in general, this approach is idiosyncratic and not feasible to deliver to [any large population] in a cost-effective manner". This is still true today. A driving factor in the cost to author tutors, deliver instruction and assess tutor effectiveness is a lack of standard definitions, knowledge representations, data structures and processes upon which modular reusable tutor components could be built. This paper discusses the potential of a GIFT to make it easier and more cost-effective for large organizations meet their broad and diverse training needs.

Interest in adaptive CBTS continues to grow internationally. The North Atlantic Treaty Organization (NATO) Training Group's working group on Individual Training and Educational Development (IT&ED) found substantial instructional efficiencies (e.g., reduced costs and enhanced effectiveness) are readily achievable through the use of computer-based tutoring technology. However, most of the benefits examined concerned "memorization, understanding, and application of relatively straightforward facts, concepts, and procedures" and were not well suited to support complex or ill-defined environments where trainees were expected to apply judgment and exercise their adaptive and creative skills.

Expectations are on the rise for CBTS to adapt to each student's learning needs during instruction. The potential is evident, but unrealized for CBTS to skillfully facilitate student motivation, engagement, workload, and emotions in much the same way as expert human tutors "read" student behaviors and language to determine their readiness to learn and then employ strategies to maintain/enhance student learning experiences.

A common CBTS ontology would go a long way toward standardizing tutor authoring methods, management of instruction in CBTS environments, the assessment of student performance/learning during instruction, and the learning effect of tutoring systems, components and technologies (tools and methods). This paper assesses current trends in adaptive and predictive computer-based tutoring ontology development, identifies gaps and discusses opportunities for future research. The intent of this paper is to introduce CBTS ontology concepts discussed in the "adaptive and predictive computer-based tutoring" track of the the Defense and Homeland Security Simulation (DHSS) Workshop 2012 that are relevant to nations who wish to exploit technologies to support tailored and adaptive training solutions.

2. INFLUENCING FACTORS IN ONTOLOGY DESIGN

The Generalized Intelligent Framework for Tutoring (GIFT) is an open source tutoring architecture being developed by the U.S. Army Research Laboratory. The intent of GIFT is to develop/integrate CBTS capabilities to: 1) facilitate authoring, 2) manage instruction, and 3) assess learning and performance.

2.1. Facilitating Authoring

The design goals for authoring processes within GIFT are listed below and have been adapted from Murray (2003):

- decrease time and cost to produce CBTS
- improve usability and decrease expertise needed to produce CBTS

- incorporate good instructional design principles
- incorporate good human-computer interaction (HCI) design principles
- incorporate good instructional principles
- allow domain experts, system designers and trainers/teachers to develop, organize and use domain knowledge to author instruction
- allow for rapid integration of domain-independent knowledge (e.g., trainee data) and components (e.g., sensors, models, modules) to author a CBTS

To facilitate authoring, the GIFT ontology accounts for five core authoring processes to support rapid/economical development of tutoring systems and components. These processes support development of: user models; domain-specific knowledge; generalized (domain-independent) instructional strategies; human-tutor interfaces and; CBTS from components. While at the writing of this paper, not all elements within GIFT are fully matured, the ontology addresses their relationships and interactions.

2.1.1. Authoring User Models

In GIFT, user models include learner models (also known as trainee models), expert models, developer models and a variety of other models according to the types of GIFT users. In developing an adaptive CBTS, a comprehensive learner model (also known as a trainee model) is the basis for tailoring training (e.g., selecting domain-specific content based on the learner's competence level or selection of instructional strategies). There are two major challenges in deciding what needs to be in the learner model: identifying what learner information is relevant to instructional decisions; and collecting that information unobtrusively so as not to interfere with the learning process (Sottilare and Proctor, 2012).

Martens and Uhrmacher (2004) defined the learner model as consisting of a learner profile and a representation of the learner's knowledge. We have adapted and expanded this learner model (LM) to be represented by learner states that include the learner's cognitive and affective states as well as their potential and performance:

$$\mathrm{LM} = \{\textit{potential, performance, cognitive, affective}\} \quad (1)$$

Potential is a measure of expected capabilities (or competence) based on the learner's historical data and their current performance. Performance is a measure of progress toward learning goals. Cognition and affect have been included in the learner model to address variables like engagement, workload and motivation which have a significant influence on learning. The learner states may be derived using computation or classification methods based on source data including data input (e.g., surveys), data capture (e.g., physiological or behavioral sensors) and historical data (e.g., learning management system records).

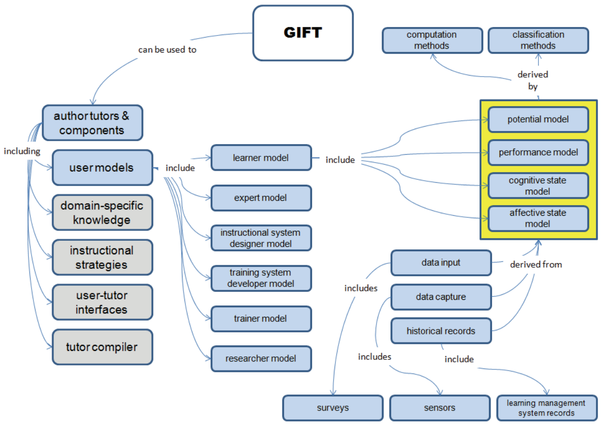


Figure 1: Authoring User Models

There are currently no standard learner models and this is a source of significant debate regarding what should and should not be included. The GIFT learner model presented above provides a flexible schema to allow changes in the future as research reveals which individual differences significantly influence learning outcomes. Ideally, a standard model would enable ease of integration by external user databases like Learning Management Systems (LMS).

It is envisioned that GIFT users will also include researchers, domain experts (also known as subject matter experts), instructional system designers, training system and courseware developers, and trainers. In this context researchers include personnel using GIFT to answer a research question and test a hypothesis, but we also include evaluators in this category, because they are also attempting to answer a question regarding the effectiveness of a component, method or system. The processes for assessing effectiveness are described later in this paper (see Section 2.3).

Domain experts are GIFT users who perform training tasks in a controlled environment and support the generation of expert models through the capture of their behaviors and decision processes. While operationally savvy, these experts may or may not have the experience needed to develop expert models on their own and must be guided by GIFT. Methods are needed to automatically capture expert behavior, feedback, decisions and reflections to construct the expert model. It may be necessary to capture data from several experts to insure a stable model. The ontology should include considerations to be adaptable to the needs of the domain expert as a user.

The same can be said for other users (instructional system designers, training system developers and trainers). Templates or user profiles will be needed to support the specific tasks conducted by these users and as for all users, the ontology should be capable of adapting to the needs and limitations of these different classifications of users.

2.1.2. Authoring Domain-Specific Knowledge

The selection or development of domain-specific knowledge should be informed by good instructional system design principles. An example includes the ADDIE model (Branson, Rayner, Cox, Furman, King, Hannum, 1975). The domain-specific knowledge discussion below is supported to a large degree by **Figure 2**. Domain-specific knowledge includes the following elements: learning objectives, media, task, conditions, performance standards, measures, common misconceptions, and a library of context-specific feedback and questions. In part, expert models inform tasks, conditions, the setting of standards, the selection of measures of performance, and common misconceptions (areas where learners are likely to have difficulty grasping domain concepts).

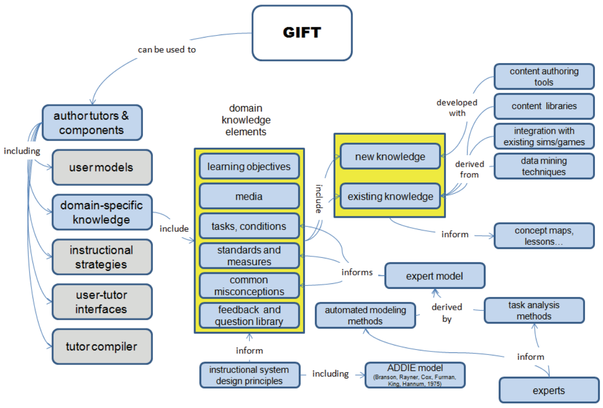


Figure 2: Authoring Domain-Specific Knowledge

A significant reduction in development time and cost might be realized by enhancing processes to reuse existing domain-specific knowledge. For instance, the cost of media development could be drastically reduced through the use of commercial games (e.g., game-based tutoring) and data mining could be used to locate appropriate shareable content objects (SCOs) on the internet to meet course development needs. SCOs may also be stored in local or server-based libraries.

If reuse is not an option, authoring tools, processes and templates are described in the ontology to support development of new knowledge. Authoring tools should be adapted to support the selection of media (e.g., interactive multimedia instruction (IMI) levels). IMI review checklist (U.S. Training and Doctrine Command Pamphlet 350-70-2, 2003) details media selection and interactivity.

2.1.3. Authoring Instructional Strategies

The search continues for a set of domain-independent strategies that will provide the optimal mix of direction and support to enhance learning and performance. Instructional strategies, tactics and strategy selection methods being evaluated for use in GIFT are based on a mix of motivational, tutoring and learning theories as shown in **Figure 3**.

Motivational theories like Maslow's hierarchy of needs (1943) are being analyzed to determine how the tutor can optimally capture the learner's interest and maintains it throughout the tutoring experience and subsequent interactions with the tutor.

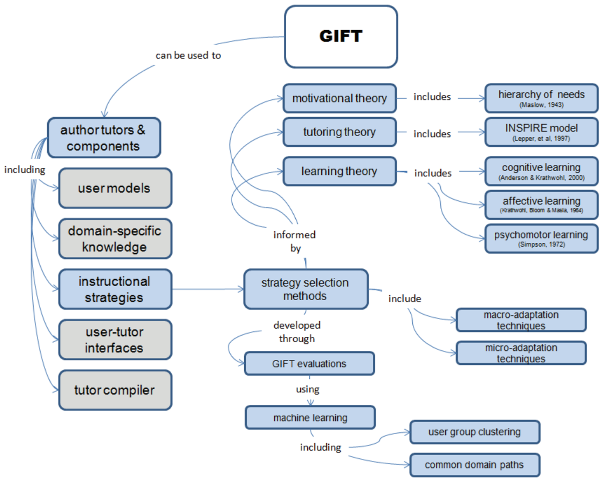

GIFT
can be used to
author tutors & components
including
user models
domain-specific knowledge
instructional strategies
user-tutor interfaces
tutor compiler
motivational theory
tutoring theory
learning theory
includes
includes
includes
hierarchy of needs (Maslow, 1943)
INSPIRE model (Lepper, et al, 1997)
cognitive learning (Anderson & Krathwohl, 2000)
affective learning (Krathwohl, Bloom & Masia, 1964)
psychomotor learning (Simpson, 1972)
informed by
strategy selection methods
include
macro-adaptation techniques
micro-adaptation techniques
developed through
GIFT evaluations
using
machine learning
including
user group clustering
common domain paths

Figure 3: Authoring Instructional Strategies

Maslow addresses motivational concepts that are relevant to learning and include social (e.g., belonging) needs, self-esteem (e.g., confidence) needs, and self-actualization.

With the objective of emulating the characteristics of the best human tutors in our CBTS, we selected tutor studies conducted by Lepper, Drake and O'Donnell-Johnson (1997) offered the most promise. Their INSPIRE tutoring model is now the subject of an empirical evaluation that will be conducted using the GIFT experimental methodology outlined in

Figure 4. This methodology is discussed in more detail in Section 2.3.

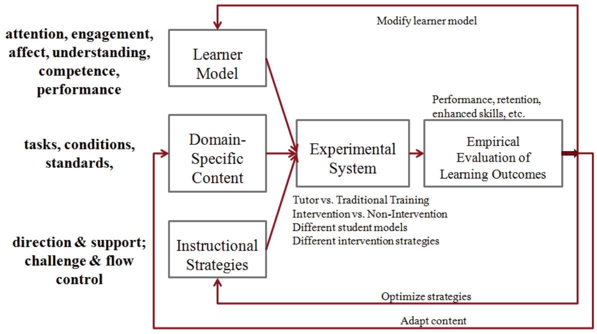

attention, engagement, affect, understanding, competence, performance
Learner Model
Modify learner model
tasks, conditions, standards,
Domain-Specific Content
direction & support; challenge & flow control
Instructional Strategies
Experimental System
Performance, retention, enhanced skills, etc.
Empirical Evaluation of Learning Outcomes
Tutor vs. Traditional Training
Intervention vs. Non-Intervention
Different student models
Different intervention strategies
Optimize strategies
Adapt content

Figure 4: GIFT Experimental Methodology

Currently, strategies are being examined that align with the class of learning (e.g., cognitive, affective, psychomotor, social, and hybrid learning) highlighted in the instructional material. In the near-term, GIFT will be focused on two major techniques to adapt experiences to the needs of the learner: macro-adaptation and micro-adaptation. Macro-adaptive techniques use historical learner data (e.g., domain performance, competency level and experience) to understand learner potential and make appropriate instructional selections (e.g., challenge level of instruction) prior to the start of instruction. Micro-adaptive techniques use current cognitive and affective states to make near-real-time decisions about instruction and feedback during the tutoring process.

2.1.4. Authoring User-Tutor Interfaces

In order to support instructional strategies, the tutor must have access to data about the user (e.g., learner, expert, and researcher). This data may come from a user model (e.g., historical data from a learner model) or it may be real-time data accessed through user-tutor interfaces (see **Figure 5**). User-tutor interfaces present sensory stimuli (e.g., visual media) and receive learner data through sensors that collect information about the behaviors and physiology of the user. Two-way communication interfaces use artificial intelligence techniques to understand and generate natural language responses.

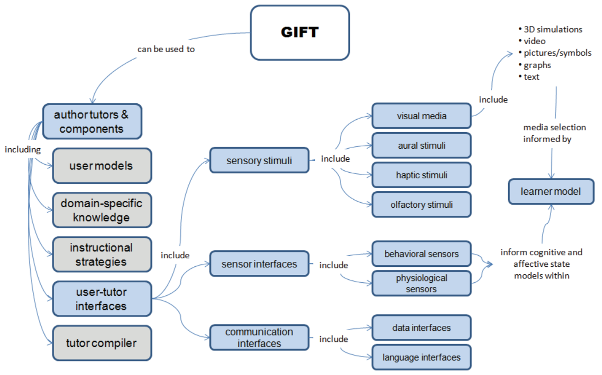


Figure 5: Authoring User-Tutor Interfaces

2.1.5. Integrating Tutor Components

An essential part of the ontology is the capability to integrate domain-dependent (e.g., domain knowledge) and domain-independent components (e.g., sensors, classification models and an instructional strategy engine) to compose a tutor for training or experimentation. As shown in **Figure 6**, GIFT system recommendations (heuristics) are informed by literature reviews and empirical research results and these in turn inform the selection of tutor module elements (e.g., clustering and classification models). The selection of trainee classification models are significantly influenced by the selection of sensors (behavioral and physiological).

2.2. Managing Instruction

This section reviews the initialization, pre-instruction, instruction, and post-instruction processes under consideration in a GIFT ontology.

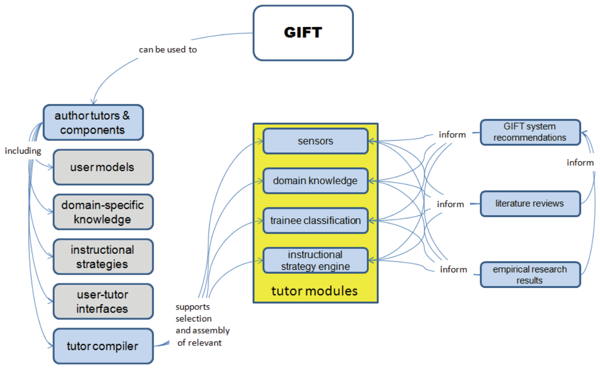


Figure 6: Tutor Compilation

2.2.1. Initialization and Pre-Instruction Phases

During the initialization phase, the user is authenticated and classified either as a learner, designer, developer, trainer or researcher. If the user is a learner, the learner model is initialized and used to inform domain knowledge selections and initialization of domain-independent modules (e.g., instructional strategy engine) within GIFT. Sensors are also initialized and verified to insure that data is being recorded. Once initialization is complete, pre-instructional activities can begin. Pre-instruction activities include pre-training surveys and a mission briefing that consists of a narrative (text or aural) to provide context and motivational support.

2.2.2. Instructional Phase

The instructional phase includes elements of the tutoring process and tutor behaviors as shown in **Figure 7**. The INSPIRE model of tutoring (Lepper, Drake and O'Donnell-Johnson, 1997; Lepper and Woolverton, 2002) is one model that could be used to moderate the CBTS decisions and feedback during instruction.

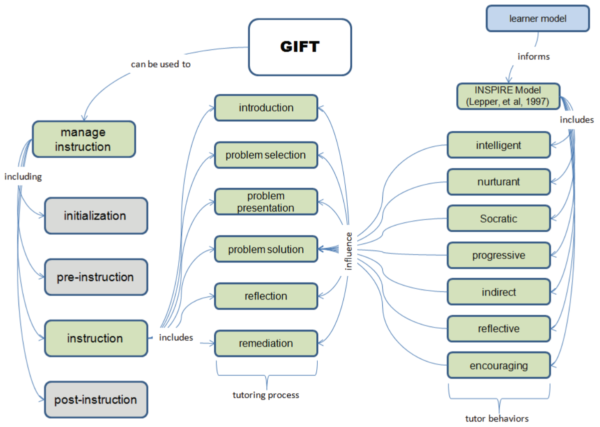


Figure 7: Tutoring Processes and Tutor Behaviors

Particular attention is paid to how tutor behaviors influence the five stages of the tutoring process. The introduction is an opportunity for the learner and the tutor to build rapport as the tutor demonstrates credibility and supportiveness by providing relevant historical information and motivational narrative.

During problem selection and presentation, the tutor also demonstrates its understanding of the problem difficulty, common misconceptions and other domain-specific knowledge to work hand-in-hand with an understanding of the learner's potential (e.g., domain competency).

During problem solution, the tutor monitors the learner's progress against expectations derived from the potential model within the learner model. Once the problem is solved, the tutor encourages the learner to reflect on the problem solving process, implications for use of this process in the future, and development of generalized models to solve similar problems. Finally, when necessary, the tutor provides ties back to foundational material to clarify misunderstood concepts.

2.2.3. Post-instruction

Once a body of instruction (e.g., a lesson) has been presented and concepts within the instruction have been mastered, the tutor begins a post-instruction process that includes a reaction assessment (what the learner thought of the training), a learning and performance assessment (to determine change in potential for future training), meaningful feedback to the trainee on their performance and their ability to generalize what was learned.

2.3. Assessment

Any CBTS ontology should be able assess improvements in learning and performance for any course or instructional subset (e.g., lesson or concept). This may be accomplished through frequent testing opportunities, but also may be assessed through other measures. For example, concept maps of the lesson could be used to delineate optimal paths based on expert modeling. For GIFT, we intend to use Markov Decision Processes to determine 'reward values' as the learner moves through each lesson and masters each concept. Increases in reward values will indicate learning while decreases in reward values will indicate potential misconceptions. The tutor will use this information in making decisions on how to bring the learner back to a learning path with a successful outcome.

The ontology should consider not only the learner performance, but also enable the assessment of tutoring methods and models across populations, and their effect on learning. For example, one research question that might be evaluated in GIFT is: what is the optimal set of variables that need to be represented in a learner model in order to make the most accurate predictions of learner states and thereby select optimal instructional strategies? To answer this question a number of variables (e.g., domain competency and historical performance) may be evaluated for their influence on learner state (e.g., cognitive or affective state) predictive accuracy using the experimental methodology outlined in **Figure 4**. Tutoring methods can also be evaluated using these methods.

3. DISCUSSION

The basis for a comprehensive CBTS ontology exists and has been evolving since the first CBTS were built over thirty years ago. The design objectives for authoring functions for CBTS are well documented (Murray, 1999; Murray, 2003; Koedinger, Aleven, Heffernan, McLaren, and Hockenberry, 2004). In addition to those frameworks already mentioned in this paper, there are several CBTS frameworks which have been proposed to address niche instructional design areas including: the evaluation of semantic knowledge during problem solving (Fournier-Viger, Nkambou, and Mayers, 2008), integration of tutoring approaches into existing collaborative applications via scripting (Harrer, Malzahn, and Wichmann, 2008), knowledge acquisition management (Riccucci, Carbonaro, and Casadei, 2005), and modeling human teaching tactics and strategies (du Boulay and Luckin, 2001). However, no framework to date has provided a comprehensive architecture to support authoring, instruction and assessment of CBTS.

What has been lacking is a methodology to assess tutoring technologies (tools and methods) and a framework to bring together best tutoring practices for authoring and instruction based on empirical experimental results. GIFT is our attempt at providing this holistic view of the CBTS problem space.

3.1. Current Trends

Few CBTS frameworks support multiple instructional approaches applicable across multiple instructional domains/topics. Most tutors employ a single strategy in a single instructional domain. AutoTutor broadly applies instructional strategies that include assessment/management of affective states (e.g., confusion and frustration) toward the goal of enhanced learning in well-defined domains (e.g., mathematics and physics). Affective learning influences how individuals manage their cognitive resources so applying strategies to enhance motivation encourages behaviors of perseverance and enthusiasm to continue when challenge is present.

3.2. Gaps

It will be critical to build upon AutoTutor's affective capabilities and extend tutoring into ill-defined domains (e.g., negotiation tasks and exercising moral judgment) experienced by military members in today's complex world. Ill-defined domains complicate the task of authoring CBTS since the linkage between specific learner actions and progress toward learning objectives is not always clear. Authoring is further complicated by the fact that there may be many more "paths to success" in ill-defined domains than in well-defined domains. This expands the number of scenario adaptations needed to represent all the possible (or likely) domain paths and increases the burden on scenario developers to provide instructional content at each node in the scenario.

In addition to being able to provide automated instruction to learners experiencing training in ill-defined tasks, researchers today are seeking capabilities to support low-cost, unobtrusive sensing of learner data (behaviors and physiological measures) to inform the cognitive and affective state classification models to determine learner states. This is an important element of the learning effect chain (**Figure 8**) where the outputs of cognitive and affective learner state models inform the selection of optimal instructional strategies to support higher learning gains (e.g., enhanced knowledge acquisition, skill acquisition, and retention). Improving the accuracy of instructional strategy selection may also be one path to accelerating learning (acquiring the same learning effect with less instructional contact time).

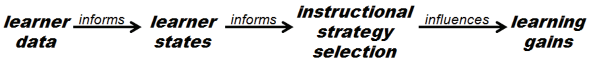


Figure 8: Learning Effect Chain

4. FUTURE WORK

GIFT will continue to evolve along the three primary vectors of authoring, instruction and assessment. Our intent is to provide GIFT as a set of tools, methods and heuristics to the user community and encourage open development that can be evaluated for inclusion in the baseline for the benefit of the user community. Research projects within the U.S. Army Research Laboratory will continue to focus on the assessment and validation of models and methods for inclusion in the GIFT baseline.

Several XML-based configuration tools are being developed to enhance the authoring capability and usability of GIFT including a learner modeling tool, a survey authoring tool, a domain knowledge file authoring tool, an event reporting tool, and experimentation support tool.

GIFT is evaluating other CBTS constructs to leverage open-source and government-developed capabilities. AutoTutor, AutoTutor Lite (web-based version of AutorTutor), and the Student Information Models for Intelligent Learning Environments (SIMILE) are three capabilities currently being assessed for inclusion in the GIFT baseline. AutoTutor and AutoTutor Lite manage tutoring experiences in multiple well-defined knowledge domains (e.g., math or physics). Additional research is needed to expand CBTS capabilities to support more ill-defined training domains (e.g., exercising moral judgment).

REFERENCES

Branson, R. K., Rayner, G. T., Cox, J. L., Furman, J. P., King, F. J., Hannum, W. H. (1975). Interservice procedures for instructional systems development. (5 vols.) (TRADOC Pam 350-30 NAVEDTRA 106A). Ft. Monroe, VA: U.S. Army Training and Doctrine Command, August 1975. (NTIS No. ADA 019 486 through ADA 019 490).

du Boulay, B. and Luckin, R. (2001). Modelling human teaching tactics and strategies. *International Journal of Artificial Intelligence in Education*, Vol 12: 235–256, 2001.

Fournier-Viger, P., Nkambou, R., Mayers., A.: A Framework for Evaluating Semantic Knowledge in Problem-Solving-Based Intelligent Tutoring Systems. In: Proc. of FLAIRS 2008, pp. 409–414. AAAI press, Menlo Park (2008)

Harrer, A., Malzahn, N. and Wichmann, A. (2008). The remote control approach - An architecture for adaptive scripting across collaborative learning environments. *Journal of Universal Computer Science*, vol. 14, no. 1 (2008), 148-173.

Koedinger, K. R., Aleven, V., Heffernan, N., McLaren, B., & Hockenberry, M. (2004). Opening the door to non-programmers: authoring intelligent tutor behavior by demonstration. In Proceedings of Seventh International Conference on Intelligent Tutoring Systems, ITS 2004 (pp. 162-174). Berlin: Springer Verlag.

Lepper, M. R., Drake, M., & O'Donnell-Johnson, T. M. (1997). Scaffolding techniques of expert human tutors. In K. Hogan & M. Pressley (Eds), Scaffolding student learning: Instructional approaches and issues (pp. 108-144). New York: Brookline Books.

Lepper, M. and Woolverton, M. (2002). The Wisdom of Practice: Lessons Learned from the Study of Highly Effective Tutors. In J. Aronson (Ed) *Improving academic achievement: impact of psychological factors on education* (pp. 135-158). New York: Academic Press.

Loftin, B., Mastaglio, T., & Kenney, P. (2004), *Outstanding Research Issues in Intelligent Tutoring Systems*, study commissioned by the Research Development and Engineering Command (RDECOM), Orlando, Florida, USA under contract N61339-03-C-0156, Retrieved from http://www.mymicsurveys.com/site/files/pub_4.pdf.

Martens, A., and Uhrmacher, A.M. (2004). A formal tutoring process model for intelligent tutoring systems. In Proceedings of the 16th *European Conference on Artificial Intelligence, ECAI 2004*, 124–128, 2004.

Maslow, A.H. (1943). "A Theory of Human Motivation," Psychological Review 50(4): 370-96.

Murray, T. (1999). Authoring intelligent tutoring systems: An analysis of the state of the art. *International Journal of Artificial Intelligence in Education*, 10(1):98–129.

Murray, T. (2003). An Overview of Intelligent Tutoring System Authoring Tools: Updated analysis of the state of the art. *Authoring tools for advanced technology learning environments*. 2003, 491-545.

Riccucci, S., Carbonaro, A., and Casadei, G. An architecture for knowledge management in intelligent tutoring system. In Cognition and Exploratory Learning in Digital Age (Porto, Portugal, December 2005), pp. 473–476.

Sottilare, R. & Proctor, M. (2012). Classifying student mood within intelligent tutoring systems (ITS). *Journal of Educational Technology*, 15 (2), 101-114.

U.S. Training and Doctrine Command (2003). Pamphlet 350-70-2 Appendix K (Checklist 9).

AUTHOR BIOGRAPHY

Robert A. Sottilare, Ph.D. is the Associate Director for Science & Technology within the U.S. Army Research Laboratory - Human Research and Engineering Directorate (ARL-HRED) and directs research within the Learning in Intelligent Tutoring Environments (LITE) Laboratory at ARL's SFC Paul Ray Smith Simulation & Training Technology Center (STTC). He has 28 years of experience in both U.S. Army and Navy training and simulation as a researcher, engineer and program manager. He leads the international program at STTC and chairs training technology panels within The Technical Cooperation Program (TTCP) and NATO. Dr. Sottilare holds a patent for a high-resolution, head-mounted projection display and his recent publications have appeared in the Educational Technology Journal, the Journal for Defense Modeling and Simulation and the proceedings of the Intelligent Tutoring Systems Conference 2010. He is a graduate of the Advanced Program Managers Course at the Defense Systems Management College, and his doctorate in modeling & simulation with a focus in intelligent systems is from the University of Central Florida. In January 2012, Dr. Sottilare was honored as the inaugural recipient of the U.S. Army Research Development & Engineering Command's (RDECOM's) Modeling & Simulation Lifetime Achievement Award. The focus of his current research is on the application of artificial intelligence tools and methods to adaptive training environments.

CRITICALITY ASSESSMENT VIA OPINION DYNAMICS

Gabriele Oliva(a), Estefania Etcheves Miciolino(b)

(a),(b) University Campus BioMedico, Via Alvaro del Portillo 21, 00128 Rome, Italy.

(a)g.oliva@unicampus.it, (b)e.miciolino@unicampus.it

ABSTRACT

In this paper a framework for merging clashing information is introduced based on the Hegelsmann and Krause opinion dynamics model, which represents the social behavior of humans taking decisions together. Such a model differs from traditional consensus models, since the group of agents tends to distribute the opinions into several clusters. With respect to the original model, where the agents were influenced by the estimations of the others provided that their difference in opinion was smaller than a global parameter, in this paper a different value of reliability is associated to each piece of information. In this way it is possible to implement an assessment framework for the criticality of the situation in a critical infrastructure or homeland security scenario based on several clashing information, taking also into account the reliability of the source.

The result is a framework able to suitably combine different pieces of information, each with a given reliability in order to derive the most likely value (i.e., the opinion that is reached by the greatest fraction of agents), by resorting to an analogy with human decision making dynamics.

Finally the possibility to apply the framework in a distributed fashion is investigated, analyzing different complex network topologies.

Keywords: Situation Assessment, Opinion Dynamics, Critical Infrastructures, Distributed Agent Based Systems.

1. INTRODUCTION

In the literature the characterization of the behavior of interacting agents that cooperate in order to reach an agreement has been widely investigated (Olfati-Saber et. al., 2007). The interaction among the agents is usually described by means of a fixed or varying network topology encoding the communication infrastructure; in this way it is possible to describe the interaction arising among entities such as in multi-robot systems or in sensor networks. While most of the studies in the literature (Olfati-Saber et. al., 2007) provide methodologies for the distributed averaging of several opinions or data, inspecting the conditions that lead to the actual average, in real contexts involving humans it is quite frequent to notice a clusterization of opinions (Groot, 1974; Leherer, 1975).

A similar behavior is expected when the criticality of a given critical infrastructure or homeland security scenario is evaluated, since there is the possibility to have spoofed/fake information, diffused by malicious attackers in order to underestimate/overestimate the actual ongoing situation. Recently, dynamic models representing such behavior, namely *Opinion Dynamics* models, gained momentum rapidly. Within such frameworks, as in consensus models, agents are assumed to interact in order to reach an agreement on their opinion. The peculiarity of these approaches is related to the topological structure of the agents interaction which is defined by the closeness in their points of view. Indeed, when studying this class of problems, it is reasonable to consider that an agreement between two agents may take place only if their opinions are sufficiently close to each other. The question arising is whether the agents will converge to a shared opinion or split into clusters. The group of agents can be very small, thus modeling the decision process of a judgment court or a team of experts, or can be very vast, thus representing the whole population of a country. In both cases it is interesting to model the process by which the opinion of the different individuals may converge to a common value or, conversely, these opinions may become fragmented, thus dividing the agents into clusters. In the literature several opinion dynamics models have been proposed (Groot, 1974; Leherer, 1975; French, 1956; Chatterjee and Seneta, 1977; Hegselmann and Krause, 2002). Among the others, the Hegelsman-Krause Model (HK), first introduced in (Hegselmann and Krause, 2002), and then further investigated in (Lorenz J., 2006; Mirtabatabaei and Bullo, 2011; Kurza and Rambaua, 2010; Constantin Moraréscu and Girard, 2010;Blondel et al., 2009; Gasparri and Oliva , 2012; Oliva et. al., 2012; Oliva, 2012) is the most widely studied. It relies on the assumption that the opinion of each agent can be represented by means of a real value, thus modeling a scoring or a vote. In this paper, the Hegelsmann-Krause opinion dynamics model, introduced to model the social behavior of humans taking decisions together, is adopted as a framework for the merging of clashing information, each characterized by a reliability value. To this end a set of agents, each holding an initial opinion, is considered and it is assumed that the single agent is influenced by the values of the others, depending on how close their opinions are (e.g., depending on the reliability). In order to obtain such result, the original HK model is slightly modified, considering a reliability value for each agent, rather than a global parameter. Specifically, the modified model assumes that an agent will not influence another one if they have very distant opinions, unless its reliability is very high; conversely, agents with close opinions will be likely to influence each other unless their reliability is remarkably small. The result is a sophisticated framework for the composition of clashing opinions, where each agent is characterized by a reliability value; the opinions of the agents will split during the evolution of the system, leading to several clusters of opinion, each characterized by the number of agents composing the cluster. The idea, therefore, is to select the opinion of the cluster with higher cardinality as the most likely estimate of the group of agents (i.e., the resulting merged value). A crucial enhancement of such a methodology is how to let a sensor network perform a distributed agreement without resorting to a central processing unit (e.g. SCADA system). This would indeed contribute to increase the local awareness of smart equipment distributed within the field of critical infrastructures such as power grids or telecommunication networks. The underlying idea, in this case is to consider agents with local computational capability, able to interact with their neighbors according to a network topology and to exchange their opinions with such neighbors. Hence, in order to provide a distributed decision algorithm, the proposed model is endowed with a network topology, showing some simulation results depending on particular complex network topologies.

The paper is organized as follows: after an overview of the Hegelsman-Krause Opinion Dynamics Model, the proposed extension is discussed, as well as the application of the framework in a distributed fashion; finally some conclusive remarks are collected.

2. H-K OPINION DYNAMICS MODEL

Let a set of N agents, each with an initial opinion, that interact mutually, influencing their points of view. In the Hegelsman-Krause (HK) model the agent's opinion is represented by real numbers. This allows to model the behavior of a team of experts that have to reach consensus on the magnitude of a given phenomenon, e.g., the expected economic loss in a given nation, or to decide a scoring, e.g., for a project funded by an institution. The key idea of the HK model is that an agent is not completely influenced by the opinions of the others, nor completely indifferent. This behavior can be obtained by letting each agent take into account the other agents standpoint to a certain extent while forming its own opinion. This implies that agents with completely different opinions will not influence each other, while some sort of mediation will occur among agents whose opinions are close enough. This process, which is iterated several times (e.g., voting sessions), can be described by means of a discrete-time model. Let $z_i(k) \in \Re$ be the opinion of i-th agent at time step k and let $z(k)=[z_1(k),\cdots,z_n(k)]^T$ be the vector of the opinions of all the agents. The i-th agent will be influenced by opinions that differ from his own no more than a given confidence level $\varepsilon \geq 0$. Hence the *neighborhood* of an agent for each time step k can be defined as:

$$N_i(k)=\left\{ j \in \{1,\ldots,N\} : \quad |z_j(k)-z_i(k)| \leq \varepsilon \right\} \qquad (1)$$

Note that, at each step k, *N_i(k)* contains the i-th agent itself. This models the fact that each agent takes into account also its current opinion to form a new one. The last ingredient of the model is the opinion influence mechanism, that is the average of the opinions in $N_i(k)$ for each agent i. Intuitively, the reader may expect that, iterating the average of the opinions, the agents will rapidly reach a consensus. Unfortunately, the HK model has a much more complex behavior. The HK dynamic model is in the form:

$$z(k+1)=A(z(k))z(k), \qquad z(0)=z_0 \qquad (2)$$

Where *A(z(k))* is the time-varying (actually state-dependent) n x n adjacency matrix whose entries $a_{ij}(k)=1/|N_i(k)|$ if $j \in N_i(k)$ and $a_{ij}(k)=0$ otherwise, where $|N_i(k)|$ is the cardinality of $N_i(k)$. An important aspect of this model is the nature of the initial opinion profiles. Two different classes are considered in the literature (Hegselmann and Krause, 2002; Mirtabatabaei and Bullo, 2011), that is: the *equidistant profile*, where $z_i(0)=(i-1)/(n-1)$ with $z_i(0) \in [0,1]$; the *random profile*, where the opinions are uniformly distributed within $[0,1]$.

Several works can be found in the literature, which attempt to characterize the properties of the HK model. In (Hegselmann and Krause, 2002) it is conjectured that for every confidence level ε there must be a number of agents n such that the equidistant profile leads to consensus (i.e., a single shared opinion for all the agents), while in (Mirtabatabaei and Bullo, 2011) it is conjectured that, for any initial opinion profile, there exists a finite time after which the topology underlying the *A(z(k))* matrix (i.e., the structure of the mutual influence among agents) remains fixed. In (Blondel et al., 2009) it is proven that, during the evolution of the system, the order of the opinions is preserved, that is $z_i(0) \leq z_j(0) \Rightarrow z_i(k) \leq z_j(k)$ for all k. Moreover it is proved that, if the initial opinion profile is sorted, the smallest opinion $z_1(k)$ is nondecreasing with time and the largest opinion $z_n(k)$ is non increasing with time. Clearly at any step k if $|z_i(k)-z_{i+1}(k)| > \varepsilon$ this remains true for any subsequent step, and the system splits into two independent subsystems. In (Dittmer, 2001; Lorenz, 2005) the stability of the dynamical model is investigated. In particular the fact the system converges to a steady opinion profile in finite time is proven in (Blondel et al., 2009). However, the fact the system might converge to a common opinion or split into clusters is still under investigation. Experimental results suggest that the number of clusters tends to increase linearly with ε, and indeed the inter-cluster distance appears to be bounded by ε (although with irregularities for a small subset of values of ε), although a formal proof of such behavior is yet to be provided.

Figure 1 shows an example of result of the HK model with n=100 agents, for different values of the parameter ε; clearly the number of clusters tends to decrease when grows.

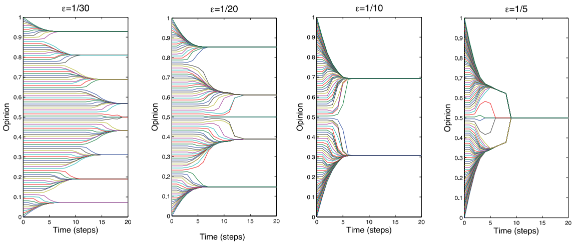


Figure 1 Simulation of Opinion Dynamics for n=100 agents and for different values of ε.

The origin of the complexity of this model is evidently the time-varying nature of the problem, and in particular the dependency on the state of the system. Note that, if the coefficients of the *A(z(k))* matrix are fixed (Groot, 1974; Leherer, 1975) the problem is significantly simplified. In order to better understand the complexity of the HK model, let us briefly discuss the difference (Gasparri and Oliva, 2012) between this model and the consensus model.

Let us consider a time-varying graph $G=\{V,E(k)\}$ with $V=\{1,\ldots,n\}$ the set of nodes and $E(k)=\{e_{ij}(k)\}\in V\times V$ the set of links at time k, and let us recall that for a discrete-time first order average consensus over $G(k)$ the dynamics of an agent i is defined as follows:

$$z_i(k+1)=z_i(k)+\tau\sum_{j\in V}\gamma_{ij}(k)\left[z_j(k)-z_i(k)\right] \qquad (3)$$

where $\gamma_{ij}(k)$ is the entry of the time varying adjacency matrix $\Gamma(k)$ of the graph *G(k)* and $\gamma_{ij}(k)=1$ if $e_{ij}(k)\in E(k)$ and zero otherwise. The parameter $\tau\in[0,1/d_{\max}(k)]$ where $d_{\max}(k)$ is the maximum degree of the graph at time k and is given by:

$$d_{\max}(k)=\max_i\{\sum_{j=1}^{n}\gamma_{ij}(k)\} \qquad (4)$$

The dynamics of the overall system is:

$$z(k+1)=[I-\tau L]z(k) \qquad (5)$$

Where *L(K)* is the Laplacian matrix of the graph *G(k)* encoding the network topology at time , whose elements $\{l_{ij}\}$ are equal to the degree *d* of node *i* if *i=j* and is equal to $-\gamma_{ij}(k)$ else.

The following lemma (Gasparri and Oliva, 2012) points out a parallelism between the two problem formulations.

Lemma 1 *Let us consider the HK model given in eq.* (2). *Then, the dynamical matrix can be restated as* $A(k)=I-D(k)L(k)$ *where L(k) is a time-varying laplacian matrix and D(k) is a diagonal matrix whose elements are* $d_{ii}(k)=1/|N_i(k)|$.

The above result emphasizes an interesting difference between consensus and opinion dynamics. For the consensus problem, the parameter τ is defined with respect to the maximum out-degree $d_{max}(k)$ of the network (over all the steps). Therefore, τ represents a global parameter common to all agents. Differently, for the HK opinion dynamics problem, there is a diagonal *D(k)* matrix of parameters where each entry $d_{ii}(k)$ is a local parameter inversely proportional to the neighborhood $N_i(k)$ of the i-th agent at time k. Finally, let us point out that for the (time-varying) consensus over a graph the convergence is related to the fact that the graph is *jointly connected* (Moshtagh and Jadbabaie, 2007) (i.e., the union of the graphs over a given time interval contains a directed spanning tree). Unfortunately, this assumption is not generally verified by the HK model due to the particular choice of the interaction policy which can lead to the isolation of some nodes, and thus to a Laplacian matrix with rows of zeros.

3. DISTRIBUTED OPINION DYNAMICS WITH HETEROGENEOUS RELIABILITY

In order to adopt the HK model as a framework for the composition and the filtering of several clashing opinions, an essential step is to modify the model in order to take into account for the reputation of each sensor. Specifically, let a reputation value $\varepsilon_i\in[0,1]$ be defined for each agent *i*, where $\varepsilon_i=1$ means completely trustworthy information and $\varepsilon_i=1$, means completely unreliable or fake information. Based on such reputation values, let us define the *neighborhood* of an agent for each time step k as follows:

$$N_i(k)=\{\ j\in 1,\ldots,n:\ \ |z_j-z_i|\le\varepsilon_j\ \} \qquad (6)$$

in this way each agent *i*, for each time step, is influenced by the opinion of an agent *j* provided that the (absolute value of the) difference in their opinions is less than the reputation value of agent *j*, hence each agent *I* evaluates the reliability of the other agents. Figure 2 shows an example of application for *N=100* agents with equispaced initial opinion profile, each with a random reputation between 1/40 and 1/9. Note that in this case the cluster with greater cardinality (42 agents) has an opinion (0.257) that is very distant from the theoretical average (0.5) and from the weighted average considering the reliability values as weights (0.479), thus modeling a complex decision process where the reliability of the information provided by each agent is considered.

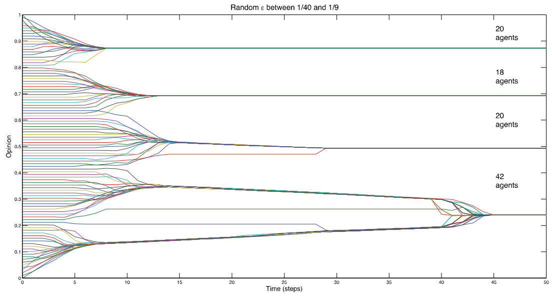


Figure 2: Simulation for n=100 agents with equispaced initial opinion profile, each with a random reputation between 1/40 and 1/9.

3.1. Distributed estimation via H-K model

The above framework is indeed a centralized framework, where the agents communicate with opinion-dependent neighborhoods, although theoretically the agents are free to communicate with each other. In order to provide a distributed framework, there is the need to endow the agents with a network topology, thus constraining the communications for an agent to the set of agents that are its neighbors according to both the network topology and the opinion differences. Let $\Gamma = \{\gamma_{ij}\}$ be the adjacency matrix that represents the topology of the network, and specifically a matrix whose coefficients $\gamma_{ij} = 1$if there is a link between agent *i* and agent *j* (we assume each $\gamma_{ii} = 1$). Let us define the neighborhood for this case as
:

$$N_i(k) = \{ \ j \in 1,\ldots,n : \quad |z_j - z_i| \le \varepsilon_j \quad \gamma_{ij} > 0 \quad \} \quad (7)$$

The following figures show some simulations for n=100 agents with equispaced initial opinion profile, each with random $\varepsilon_i \in [\ 1/100, \ \ 1/10\ ]$, over different complex network topologies (considering the same reliabilities along the different simulations).

Figure 3 shows a simulation over an Erdos-Renyi random network with a maximum of *m=10* link per node; in this case the agents tend to spread in several opinions and the cluster with higher cardinality has 9 agents and has a value of 0.27.

Figures 4 and 5 show a simulation over a Scale-free network with a maximum of m=5 and m=10 links per node, respectively; in this case it is possible to notice few clusters of high cardinality and several clusters with small cardinality (indeed Scale-free networks have few highly connected hubs and many nodes with few links). In the first case (e.g., m=5, see Figure 4) the cluster with higher cardinality (31 agents) has a value of 0.14, while in the second case (e.g., m=10, see Figure 5) the value is 0.15 and the cardinality is 29.

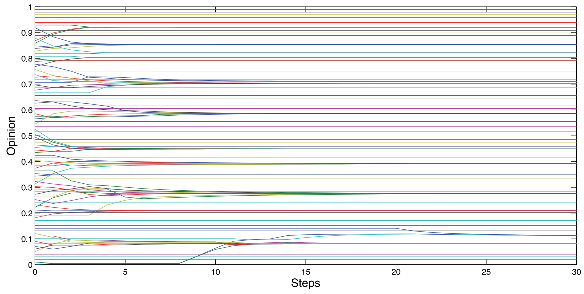


Figure 3 Simulation for n=100 agents with equispaced initial opinion profile, each with a random reputation between 1/00 and 1/10, over a random topology where a maximum of m=10 links were allowed.

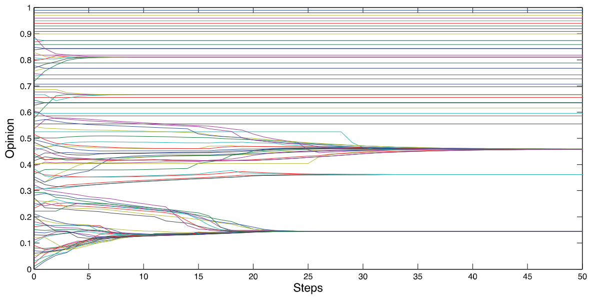


Figure 4: Simulation for n=100 agents with equispaced initial opinion profile, each with a random reputation between 1/100 and 1/10, over a Scale-free topology where a maximum of m=5 links were allowed.

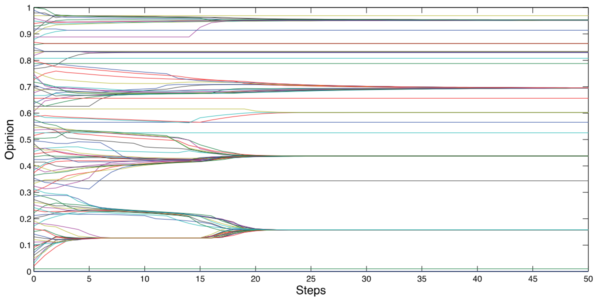


Figure 5: Simulation for n=100 agents with equispaced initial opinion profile, each with a random reputation between 1/100 and 1/10, over a Scale-free topology where a maximum of m=10 links were allowed.

As shown in Figure 6 and 7, the situation is different when a Small-world network is adopted (e.g., a lattice with rewiring probability p=0.3). Specifically Figure 6 depicts a scenario where a maximum of m=5 links is allowed for each agent, while in Figure 7 m=10 links are allowed. In this case few clusters are obtained, and the time required for obtaining a steady state is inversely dependent on the number m of maximum links per node. Notice that in this case the largest cluster coincides (the value obtained is 0.18 and the cardinality is 35 for both Figure 6 and 7).

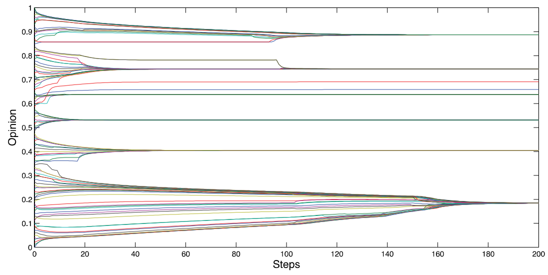


Figure 6: Simulation for n=100 agents with equispaced initial opinion profile, each with a random reputation between 1/100 and 1/10, over a Small-world topology (a lattice with rewiring probability p=0.3) where a maximum of m=5 links was allowed.

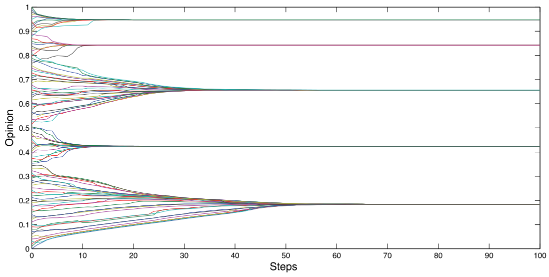


Figure 7: Simulation for n=100 agents with equispaced initial opinion profile, each with a random reputation between 1/100 and 1/10, over a Small-world topology (a lattice with rewiring probability p=0.3) where a maximum of m=10 links was allowed.

4. CONCLUSIONS

In this paper a framework for the composition of pieces of information with heterogeneous reliability that mimics the human decision-making process has been provided extending the Hegelsmann-Krause opinion dynamics model. The framework has been also extended in order to consider network topologies and therefore a distributed process. Future work will be devoted to compare such model with other approaches for sensor fusion and information merging existing in the literature. In particular, since each agent has a single initial opinion, the method is expected to be less descriptive than Dempster-Shafer Evidence Theory framework (Dempster, 1967), where each agent provides a belief in the power set of the possible hypotheses. To solve this issue future work will investigate the extension of the framework to interval opinions and to fuzzy opinions, adopting the framework in (Gasparri and Oliva, 2012; Oliva et. al., 2012; Oliva, 2012). Another issue yet to be solved is how to adopt such system in a distributed way and specifically how to select the cluster with higher cardinality in a distributed way, since each node would assume a final opinion without knowing the opinions of the other clusters. As a matter of fact, the network of distributed agents split into several clusters of opinions: however, being the agents interconnected by means of a network topology a max-consensus may be setup in order to spread the value of the cluster with greater cardinality.

ACKNOWLEDGMENTS

This work was partially supported by the European Commission, Directorate, General Home Affairs, within the Specific Programme on Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risk Programme, under Grant Home/2010/CIPS/AG/033 REFIRE - REference implementation of interoperable indoor location & communication systems for FIrst REsponders (http://www.refire.org).

REFERENCES

Blondel V., Hendrickx J., and Tsitsiklis J., 2009. On Krause's multi-agent consensus model with state-dependent connectivity, *Automatic Control, IEEE Transactions on*, vol. 54, no. 11, pp. 2586–2597.

Chatterjee S. and Seneta E., 1977, Toward consensus: some convergence theorems on repeated averaging. *J. Appl. Prob.*, vol. 14, pp. 89–97.

Constantin Morarescu I. and Girard A., 2010. Opinion Dynamics with Decaying Confidence: Application to Community Detection in Graphs, *Transaction on Automatic Control*.

Dempster A.P., 1967. Upper and lower probabilities induced by a multivalued mapping, *The Annals of Mathematical Statistics*, vol. 38, no. 2.

Dittmer J.C., 2001. Consensus formation under bounded confidence, *Nonlinear Analysis-Theory Methods and Applications*, vol. 47, no. 7, pp. 4615–4622.

French J. R. P., 1956. A formal theory of social power, *Psychological Review*, vol. 63, pp. 181–194.

Gasparri A. and Oliva G., 2012. Fuzzy opinion dynamics, *American Control Conference 2012 (ACC2012),*.

Groot M. H. D., 1974. *Reaching a consensus*. Wiley.

Hegselmann R. and Krause U., 2002. Opinion dynamics and bounded confidence models, analysis, and simulation, *Journal of Artifical Societies and Social Simulation (JASSS) vol*, vol. 5, no. 3.

Kurza S. and Rambaua J., 2010. On the hegselmann-krause conjecture in opinion dynamics, *Journal of Difference Equations and Applications*, vol. 17, no. 6, pp. 859–876.

Leherer K., 1975. *Social consensus and rational agnoiology*. Wiley.

Lorenz J., 2005. A stabilization theorem for continuous opinion dynamics, *Physica A*, vol. 355, no. 1, pp. 217–223.

Lorenz J., 2006. Consensus strikes back in the Hegselmann-Krause model of continuous opinion dynamics under bounded confidence, *Journal of Artificial Societies and Social Simulation*, vol. 9, no. 1, p. 8.

Mirtabatabaei A. and Bullo F., 2011. Opinion Dynamics in Heterogeneous Networks: Convergence Conjectures and Theorems, *Arxiv preprint arXiv:1103.2829*, no. March, pp. 1–22.

Moshtagh N. and Jadbabaie A., 2007. Distributed geodesic control laws for flocking of nonholonomic agents, *IEEE Transactions on Automtic Control*, vol. 54, no. 4, pp. 681 – 686.

Olfati-Saber R, Fax J. A. and Murray R. M., 2007. Consensus and cooperation in networked multi-agent systems, *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233,

Oliva G., 2012. Stability and Levelwise Representation of Discrete-time Fuzzy Systems, International Journal of Fuzzy Systems, vol. 14, n.2, pp. 185-192.

Oliva G., Panzieri S. and Setola R., 2012. Distributed synchronization under uncertainty: A fuzzy approach, Fuzzy Sets and Systems, vol. 206 pp. 103–120.

SITUATION AWARENESS IN CRITICAL INFRASTRUCTURES

Abate Vincenza [(a)], Adacher Ludovica [(b)], Pascucci Federica [(c)]

Dip. di Informatica e Automazione
Università degli Studi Roma Tre
Via della Vasca Navale, 79
00146 Roma, Italy

(a) abate@dia.uniroma3.it, (b) adacher@dia.uniroma3.it, (c) pascucci@dia.uniroma3.it

ABSTRACT

The present paper provides a comprehensive review about the main concepts on situation awareness for critical infrastructure. The issues related to models and architectures for data fusion and situation awareness are reported in the framework of Critical Infrastructure Protection.

Both data fusion and situation swareness have been developed in Critical Infrastructure field to merge and integrate data from several heterogeneous sensors. Since Critical Infrastructures are interconnected, the integration of sensor data is mandatory to avoid or mitigate risk of cascading and domino effects. This integration requires the cooperative signal processing of a federation of critical infrastructures.

Keywords: Situation awareness, Critical Infrastructure Protection, Distributed DF, Multi Agent System

1. INTRODUCTION

Situational Awareness (SA) refers to the ability to observe, assimilate and make predictions about relevant elements and attributes of an environment in order to provide a robust survival. SA points at *knowing what is going on around you*. In this perspective, the key idea is to exploit the knowledge acquired in the past to identify, analyze and understand the actual situation. Moreover Sa is able to forecast the evolution of a phenomena and evaluate risks. The ability to predict or model and visualize how the circumstances of a pending or evolving emergency may change over specific times allows emergency managers to allocate resources to priority areas before further damage or loss of life occurs. An effective management of crisis is essential when the emergency occur on a Critical Infrastructure (CI).

Societies are increasingly dependent on a set of products and services including the CIs, i.e. *an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*. CIs comprise essential components of industry, energy generation, security, defense, transportation and public services. In this sense, an unexpected event on CI has serious consequences to citizens and the society as a whole. The emergency management on a CI should have full situational awareness on the state of CI itself and on the responsibilities to protect them. The main concern with the CI is their growing complexity. This is partially caused by their growing interconnectedness, leading to infrastructural interdependencies with unpredictable consequences and risks. To this end, the integration of sensor data to avoid or mitigate risk due to cascading and domino effects is mandatory. This *process of combining data to refine state estimates and predictions* is known as Data Fusion (DF).

The models and architectures to describe the SA context are recalled in Sec. 2. Section 3 presents a brief background on several computational intelligence techniques applied in CIs domain. A survey on principal concepts and techniques for SA in CIs are also reported. Finally, some concluding remarks are drawn.

2. MODELS AND ARCHITECTURE FOR SITUATION AWARENESS

To describe DF systems, we first highlight the main differences between (Elmenreich 2001):

- *Models* are the description of a set of processes. This set of processes should be undertaken before the system may be regarded as fully operational.
- *Architectures* are the physical structure of the system. Particular attention is devoted to the implementation for information and data communication.
- *Frameworks* are a set of axioms and a reasoning system for manipulating entities. Examples of frameworks currently used in DF are probabilistic reasoning, possibility reasoning and evidential reasoning

2.1. Models

In the following some models proposed in literature are reported (Durrant-Whyte and Henderson 2008).

The Intelligence Cycle involves both information processing and information fusion. It is a conceptual model showing how intelligence operations are conducted.

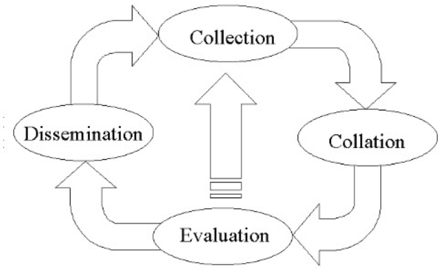


Figure 1: The Intelligence Cycle Model

It consists of four phases:

- *Collection* assets how electronic sensors or human derived sources are deployed to obtain raw intelligence data.
- *Collation* describes how associated intelligence reports are correlated and brought together.
- *Evaluation* explains how the collated intelligence reports are fused and analyzed.
- *Dissemination* clarifies how the fused intelligence is distributed to the users and who use the information to make decisions regarding their own actions and the required deployment of further collection assets.

The Joint Directors of Laboratories Model (JDL) is a layered hierarchical model that identifies fusion processes, processing functions, and processing techniques to accomplish the primary DF functions (Hall and Llinas 2008).

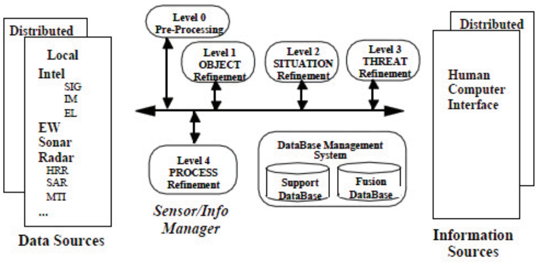


Figure 2: The Joint Directors of Laboratories (JDL) Model

The elements of the model are described in the following:

- *Sources* provide information from a variety of data sources, like sensors, a priori information, databases, human input.
- *Source preprocessing (Level 0):* The task of this element is to reduce the processing load of the fusion processes by prescreening and allocating data to appropriate processes.
- *Object refinement (Level 1):* This level performs data alignment (transformation of data to a consistent reference frame and units), association (using correlation methods), tracking actual and future positions of objects, and identification using classification methods.
- *Situation refinement (Level 2):* The situation refinement attempts to find a contextual description of the relationship between objects and observed events.
- *Threat refinement (Level 3):* This processing level tries to draw inferences about vulnerabilities and opportunities for operation on the basis of a priori knowledge and predictions about the future situation.
- *Process refinement (Level 4):* Level 4 is a meta process that monitors system performance and reallocates sensor and sources to achieve particular mission goals.
- *Database management system:* The task of the database management system is to monitor, evaluate, add, update, and provide information for the fusion processes.
- *Man-machine interaction:* This part provides an interface for human input and communication of fusion results to operators and users.

The Boyd control cycle or OODA loop possesses four phases as shown in Figure 3 (Shahbazian, Blodgett, and Labbé 2001).

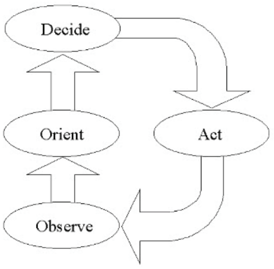


Figure 3: The Boyd (or OODA) Loop

- *Observe:* This stage is broadly comparable to source pre-processing in the JDL model (level 0) and part of the collection phase of the intelligence cycle.
- *Orient:* This stage encompasses the functions of the levels 1, 2 and 3 of the JDL model. It also includes the structured elements of collection and the collation phases of the intelligence cycle.
- *Act:* has no direct analogue in the JDL model and is the only model that explicitly closes the loop by taking account of the effect of decisions in the real world.
- *Decide:* This stage includes JDL level 4 (process refinement and resource management) and the dissemination activities of the intelligence community. It also inclues planning.

A representation of *Waterfall Model* is shown in Fig. 4. It can be seen from this figure that the flow of data operates from the data level to the decision making level. The sensor system is continuously updated with feedback information arriving from the decision-making module. The feedback element advises the multi-sensor system on re-calibration, re-configuration and data gathering aspects

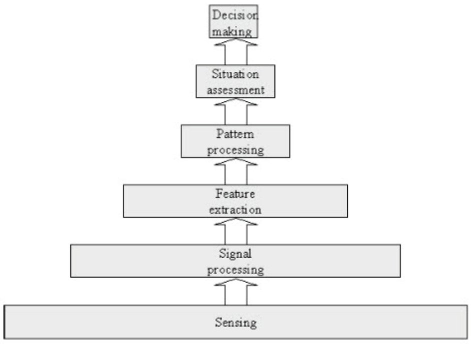


Figure 4: The Waterfall DF Process Model

The Dasaranthy Model is based on fusion functions rather than tasks and it may therefore be incorporated in every fusion activities. Many researchers have identified the three main levels of abstraction during the DF process as being:

- *Decisions* symbols or belief values
- *Features* or intermediate-level information
- *Data* or more specifically sensor data

Bedworth and O'Brien have presented the *Omnibus Model in 1999*. Figure 5 depicts the architecture of the Omnibus Model. It defines a process order and it makes explicit the cyclic nature. The model is intended to be used multiple times in the same application recursively at two different levels of abstraction. First, the model is used to characterize and structure the overall system. Second, the same structure is used to model the single subtasks of the system.

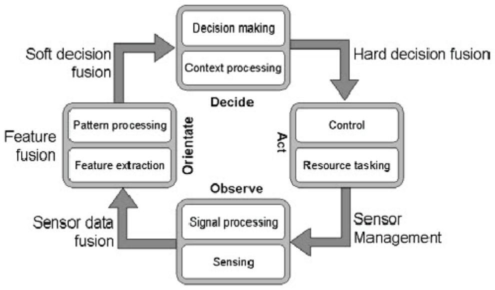


Figure 5: The Omnibus Model: A Unified DF Process Model

The Extendend OODA Model for DF systems developed at Lockheed Martin Canada (LMC) synthesizes some of the useful features of the models described previously, moreover provides a mechanism for multiple concurrent and potentially interacting DF processes. The details of the Extended OODA model are depicted in Fig. 6.

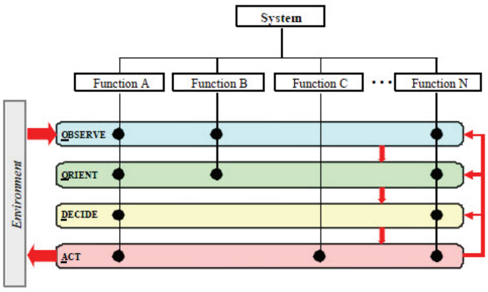


Figure 6: The Extended OODA Model for DF

A system using DF for decision-making is decomposed into a meaningful set of high-level functions (Figure 6 shows a set of N functions). These functions are examined in terms of the *Observe*, *Orient*, *Decide*, and *Act* decision loop that constitute the OODA model.

Endsley's Model defines SA as a state of knowledge resulting from a process. Situation Awareness is formally defined as *the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and projection of their status in the near future*. The model proposed by Endsley is graphically described as follows:

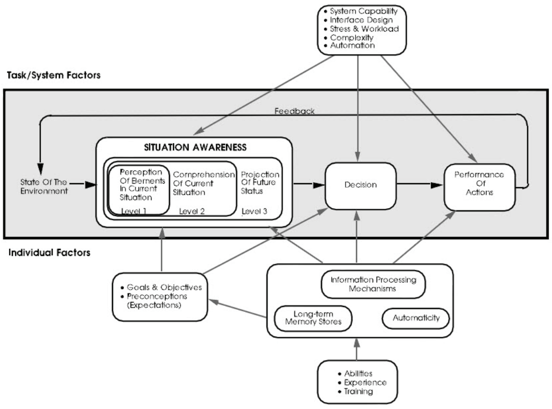


Figure 7: Endsley's Situation Awareness Model

The core portion follows Endsley's proposition that SA has three levels of mental representation:

- *Level 1 SA - Perception of the elements in the environment.* The first step in achieving SA is the perception of the status, attributes, and dynamics of relevant elements in the environment.
- *Level 2 SA - Comprehension of the current situation.* Comprehension of the situation is based on a synthesis of disjointed Level 1 elements.
- *Level 3 SA - Projection of future status* is the ability to project the future actions of the elements in the environment, at least in the

near future. It is the third and highest level of situation awareness.

The Boyd Control Loop was first used for modeling the military command process, but has since been widely used for DF. The Boyd and JDL models show distinct similarities, although the Boyd model makes the iterative nature of the problem more explicit.

The Waterfall Model emphasizes the processing functions on the lower levels. The stages relate to the levels 0, 1, 2, and 3 of the JDL model as follows: sensing and signal processing correspond to source preprocessing (level 0), feature extraction and pattern processing match object refinement (level 1), situation assessment is similar to situation refinement (level 2), and decision making corresponds to threat refinement (level 3).

In literature the JDL model is adopted to solve the SA problem. In fact, the JDL model is a suitable manner to model, describe and understand various activities in the SA community. Although the JDL provides a functional model for the DF process, it does not model it from a human perspective. Endsley provides an alternative to the JDL model that addresses SA from this viewpoint.

2.1.1. Architectures

Different architecture has been proposed in literature for DF and SA (Salerno 2001).

Centralized DF (CDF) is characterized by a hierarchy of nodes: all information is passed up the hierarchy to a centralized fusion node. An example of this kind of architecture is given in the Fig. 8.

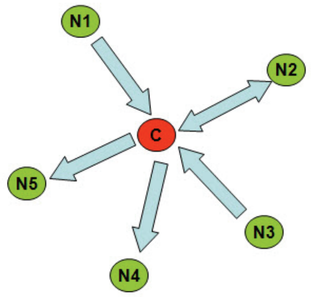


Figure 8: An Example of a Centralized DF system. The central node, C, receives information from three sensor nodes, N1, N2 and N3. It fuses information about the tracking object, thereafter it propagates back the results of DF to every node (including N2).

Unfortunately, this kind of architecture presents several disadvantages. For these reasons it is less used. Indeed,

- It imposes a latency on the availability of the fused picture at the lower level nodes;
- It also imposes a single point of failure in the system: if the fusion node is lost or loses communications, the overall situation awareness of the system is compromised;
- It limits the ability of the individual participants to operate independently or as part of a much smaller group;
- It requires significant communications bandwidth.

Decentralized DF (DDF) architectures are fully decentralized structures, without any central processor and/or common communication system. In this architecture, nodes can operate in a fully autonomous fashion, only coordinating through the anonymous communication information. Referring to Fig. 9, a DDF system consists of a network of agents, each one having its own processing capabilities, not requiring any central fusion or central communication facility.

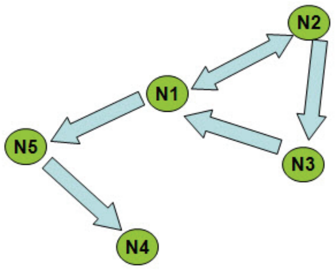


Figure 9: An example of Decentralized DF System. The agents communicate information among each other

A DDF system is characterized by three constraints:

1. There is no single central fusion center;
2. There is no common communication facility;
3. Sensor nodes do not have any global knowledge of sensor network topology.

The above constraints provide a number of important characteristics for DDF systems.

Hierarchical DF (HDF) architecture is a hybrid architecture mixing together the centralized and decentralized architectures.

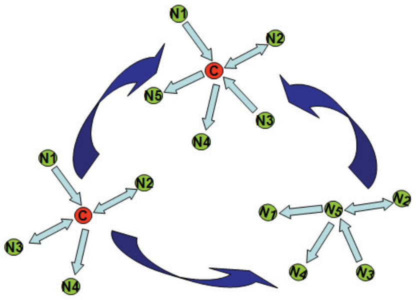


Figure 10: An Example of Hierarchical DF System. The agents are grouped in cliques and they share information about the environment with their neighbors. Communication with other groups ensures the spread of knowledge within all nodes.

In the hierarchical architecture there are often several hierarchical levels where the top level contains a single centralized fusion node and last level is made up of several decentralized (local) fusion nodes. Each local fusion node receives inputs either from a small group of sensors or from an individual sensor. The hierarchical approach has been employed in a number of DF systems and has resulted in a variety of useful algorithms for combining information at different levels of a hierarchical structure.

3. SITUATION AWARENESS IN INTERDEPENDENT SYSTEMS

Modern CI systems utilize intelligent embedded devices, communication capability, and distributed computing to streamline and fortify their operation (Kokar, Matheus and Baclawski 2009). Identifying, understanding, and analyzing such interdependencies are significant challenges (Pederson, Dudenhoeffer, Hartley and Permann 2006; Rigole and Deconinck, 2006). These challenges are greatly magnified by the breadth and complexity of transnational critical infrastructures. Examples include smart grids and intelligent water distribution networks. The increasing prevalence and complexity of this intelligent control brings its dependability into question. In this section we present several of the most established methodologies for the aggregation of multiple information sources necessary to describe a situational awareness problem for CI system.

Evidence Theory: Dempster-Shafer Theory (DST) is a mathematical theory of evidence. In a finite discrete space, Dempster-Shafer theory can be interpreted as a generalization of probability theory where probabilities are assigned to sets as opposed to mutually exclusive singletons. In traditional probability theory, evidence is associated with only one possible event. It has uncertainty management and inference mechanisms analogous to our human reasoning process.

It is based on two ideas: the idea of obtaining degrees of belief for one question from subjective probabilities for a related question, and Dempster's rule for combining such degrees of belief when they are based on independent items of evidence (Rakowsky 2007). Principally we can define three important functions in Dempster-Shafer theory:

- *the basic probability assignment function (bpa)* defines a mapping m of the power set to the interval between 0 and 1, where the bpa of the null set is 0 and the summation of the bpa's of all the subsets of the power set is 1.

$$m : P(X) \to [0,1]$$

$$m(\varnothing) = 0$$

$$\sum_{A \in P(X)} m(A) = 1$$

where *P(X)* represents the power set of *X*, ∅ is the null set, and *A* is a set in the power set (*A*∈*P*(*X*)).

- *the Belief function (Bel)* is defined as the sum of all the basic probability assignments of the proper subsets (*B*) of the set of interest (*A*) (*B*⊆*A*)

$$Bel(A) = \sum_{B|B \subseteq A} m(B)$$

- *the Plausibility function (Pl)* is the sum of all the basic probability assignments of the sets (*B*) that intersect the set of interest (*A*) (*B*∩*A*≠∅)

$$Pl(A) = \sum_{B|B \cap A \neq \varnothing} m(B)$$

Hidden Markov Model is a technique suitable for situation awareness (Thyagaraju 2010). SA is a process that comes to a conclusion based on the events that take place over a period of time across a wide area. Hence, since the situational awareness is achieved based on the sequence of events observed, Hidden Markov model (HMM) is ideally suited. The formal definition of a HMM consists of a compact notation to indicate the complete parameter set of the model:

$$\lambda = (A, B, \pi)$$

where:

A={a_{ij}} is the transition array, storing the probability of state *j* following state *i*

$$a_{ij} = P(q_t = s_j \mid q_{t-1} = s_i), \quad 1 \le i \quad , j \le N$$

B={$b_j(k)$} is the observation array, storing the probability of observation *k* being produced from the state *j*, independent of *t*

$$b_j(k) = P(x_t = v_k \mid q_t = s_j), \quad 1 \le j \le N, \quad 1 \le k \le M$$

π=π_i is the initial state distribution

$$\pi_i = P(q_1 = s_i), \quad 1 \le i \le N,$$

The model il based on two assumptions:

Markov assumption: the current state is dependent only on the previous state, this represents the memory of the model:

$P(q_t \mid q_1^{t-1}) = P(q_t \mid q_{t-1})$

Independence assumption: the output observation at time *t* is dependent only on the current state, it is independent of previous observations and states:

$P(o_t \mid o_1^{t-1}, q_1^t) = P(o_t \mid q_t)$

There are three fundamental problems that we can solve using HMMs:

Evaluation: Given the observation sequence $O=O_1O_2\cdots O_T$ and a model λ=(*A*,*B*,π), how do we efficiently compute *P*(*O*|λ), the probability of the observation sequence?

Decoding: Given the observation sequence $O=O_1O_2\cdots O_T$ and the model λ=(*A*,*B*,π), how do we choose a corresponding optimal state sequence $Q=q_1q_2\cdots q_T$ (i.e., the best "explains" the observations)?

Learning: How to maximize *P*(*O*|λ) by the model parameter λ=(*A*,*B*,π) (transitional probabilities, observation probabilities, initial probabilities))?

Artificial Neural Network (ANN) constitutes a well-established computational model, which is inspired by the biological neural system (Yao and Islam, 2008). A set of *neurons* or *processing elements,* interconnected by a network with a certain topology, has limited or local computation capability. The underlying idea is to train the network by a suitable set of known inputs and associated outputs. Thereafter, the trained network, in a "black-box" perspective, evaluates the function. Formally, an Artificial Neural Network can be defined as follow:

Definition 1 *ANN is a network of n interconnected neurons described by a directed graph* $\mathcal{G}=\{\mathcal{V},\xi,\mathcal{W}\}$ *where* $\mathcal{V}=\{1,\cdots,n\}$ *is the set of nodes/neurons and* $\xi\xi=\{e_{ij}\}\in\mathcal{V}\times\mathcal{V}$ *is the set of links; the weight of the link* e_{ij} *is described by the entry* w_{ij} *of the adjacency matrix* $\mathcal{W}$.

The structure of an ANN is typically composed by four sets:

- The set of processing units or neurons;
- The weighted links between the processing units;
- The activation rule, that converts the neuron's inputs into its outputs;
- The learning mechanisms to adjust the weights.

The focus is on the learning procedure used to train the ANN. Several methodologies are used, according to a supervised or unsupervised learning approach.

Agent-based Modeling A new emerging modeling paradigms is Multi Agent Systems (Dianne, Barton and Stamber 2000). These agent-based systems try to tackle a variety of complex problems using a fully distributed, bottom-up approach using a society of autonomous, interconnected, intelligent agents. Agent-based models are frequently used in interdependency and infrastructure analysis. Infrastructure or physical components are modeled as agents, allowing analysis of the operational characteristics and physical states of infrastructure. The agents are able to capture rational and non-rational behavior. We can define an agent as

Definition 2 *An autonomous agent is a system situated within and a part of an environment that senses that environment and acts on it, over time, in pursuit of its own agenda and so as to affect what it senses in the future.*

A CI is characterized by its location, its behaviour, interaction capabilities and its internal state. Then a CI can be modeled as an autonomous agent. The system composed by interdependent CI can be modeled as interacting agents cooperating and/or competing to realize a common or an individual goal.

Interactions between agents are the following:

- Agents have the ability to co-operate or to act against the interest of other agents
- Agents can interact whilst having different level of information about each other ;
- Agents may interact in singular encounters, or their interactions and negotiations may take place over multiple rounds of engagement;
- Decisions and actions of agents can be reached simultaneously, or can occur sequentially.

4. CONCLUSION

As we have seen there is a growing interest in critical infrastructure protection, situation awareness, and the risks related to the increasing interconnection of these infrastructures. To assess these risks new modeling and simulation tools are needed; many modeling frameworks have been proposed in the recent years. This paper proposes a descriptive survey on this great variety of approaches, considering both high-level macroscopic models and microscopic models. These two different perspectives meet in the agent-based approach that seems to be a promising technique, even if its practical use in the field of critical infrastructures is yet to be proven. In the field of SA for CI the techniques adopted should be considering the "man in the loop" problem, by modeling reasoning about ignorance, spatial-temporal reasoning capabilities, and social ability for acquiring information, hence HMM, ANN, and Evidence Theory seems to be suitable approaches.

According with these remarks, future work will address a theoretical foundation of situation awareness and its measurement based on dynamic decision networks and information value theory.

REFERENCES

Dianne, C. Barton, K., Stamber, L., 2000. An Agent-Based Microsimulation of Critical Infrastructure Systems, *Proceedings of the 8th International Energy Forum*, Las Vegas.

Durrant-Whyte, H.F., Henderson, T.C., 2008. Multisensor Data Fusion. In *Springer Handbook of Robotics*, Siciliano, B, and Kathib H. Eds, 585-610.

Elmenreich, W., 2001. *An Introduction to Sensor Fusion Research.* Report 47/2001, Institut fur Technische Informatik.

Hall, D.L., Llinas, J., 2008. *Handbook of Multisensor Data Fusion*, CRC press. Lopez, J., Setola, R., Wolthusen, S.D., (Eds), 2012. *Critical Infrastructure Protection, Information Infrastructure Models,* Lecture Notes in Computer Science, Analysis and Defence, Springer.

Kokar, M.M., Matheus, C.J., Baclawski, K., 2009. Ontology-based situation awareness. *Inf. Fusion*, 10(1), 83-98.

Pederson, P., Dudenhoeffer, D., Hartley, S., Permann, M., 2006. *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Rep.No INL/EXT-06-11464, Critical Infrastructure Protection Division, INEEL.

Rakowsky, U., 2007. *Fundamentals of Dempster-Shafer theory and its applications to system safety and reliabilitymodeling*. RTA, No. 3-4.

Rigole, T., Deconinck, G., 2006. A Survey on Modeling and Simulation of Interdependent Critical Infrastructures, *Proceeding of the 3rd IEEE BENELUX Young Researchers Symposium in Electrical Power Engineering*, Ghent, Belgium.

Salerno, J., 2002. Information Fusion: A High-level Architecture Overview*, Proceedings of the Fusion-2002*, pp. 680-686, Annapolis, MD.

Shahbazian, E., Blodgett, D.E., Labbé, P., 2001. The Extended OODA Model for Data Fusion Systems. *Proceedings of the 4th International Conference on Information Fusion*, pp.1-19, Montréal.

Thyagaraju, D., 2010. *Hidden Markov Model as a Framework for Situational Awareness, Sensor Fusion and its Application*s, Ciza Thomas (Ed.).

Yao, X., Islam, Md.M., 2008. Evolving artificial neural network ensembles, *IEEE Computational Intelligence Magazine*, 3(1), 31-42.

DETECTION OF AND REACTION TO CYBER ATTACKS IN A CRITICAL INFRASTRUCTURES SCENARIO: THE COCKPITCI APPORACH

Donato Macone[(a)], Francesco Liberati[(a)], Andrea Simeoni[(a)], Francesco Delli Priscoli[(a)], Marco Castrucci[(a)], Stefano Panzieri[(b)], Serguei Iassinovski[(c)], Michele Minichino[(d)], Ester Ciancamerla[(d)]

[(a)]Università di Roma "Sapienza", V. Ariosto 25, Rome, 00185, Italy
[(b)]Università degli Studi Roma Tre, Via della Vasca Navale 79, Rome,00146,Italy
[(c)]Multitel ASBL, Rue Pierre& Marie Curie 2, Mons, 7000, Belgium
[(d)]ENEA,Lungotevere Thaon di Revel, 76, Rome, 00196, Italy

[(a)]{macone, liberati, asimeoni, dellipriscoli, castrucci}@dis.uniroma1.it, [(b)]panzieri@dia.uniroma3.it,
[(c)]iassinovski@multitel.be, [(d)]{ester.ciancamerla, michele.minichino}@enea.it

ABSTRACT

The protection of the national infrastructures is one of the main issues for national and international security. The FP7 MICIE project has achieved promising results by developing a secure online software architecture and by sharing information on a real time basis among local risk predictors, in order to obtain accurate and synchronized predictions using shared interdependency models. However, results of MICIE project are not enough in order to quickly and effectively react to all adverse events that may occur over the System of Systems and, in particular, to face cyber attacks. The EC FP7 CockpitCI project aims to improve the resilience and the dependability of CIs through the design and the implementation of an Alerting System that provides to CI operators an efficient tool to support them: (i) in the prevention of cyber attacks and (ii) in the implementation of consequence containment strategies in case of attack.

Keywords: Critical Infrastructure protection, SCADA systems, cyber attacks countermeasures, detection and reaction strategies.

1. INTRODUCTION

The protection of the national infrastructures (i.e. the System of Systems including energy grids, transportation networks, telecommunications systems, etc., Suter and Brunner (2008)) is one of the main issues for national and international security. There are, in principle, several approaches that should be used to this end that encompass analytical (Bobbio, Bonanni, Ciancamerla, Clemente, Iacomini, Minichino, Scarlatti, Terruggia and Zendri, 2010;Bobbio, Ciancamerla, Diblasi, Iacomini, Mari, Melatti, Minichino, Scarlatti, Terruggia, Tronci and Zendri, 2009), simulative (Ciancamerla, Foglietta, Lefevre, Minichino, Lev and Shneck, 2010; Ciancamerla, Di Blasi, Foglietta, Lefevre, Minichino, Lev and Shneck, 2010) and what-if analyses (Haimes, Horowitz, Lambert, Santos, Lian and Crowther, 2005; De Porcellinis, Panzieri, Setola and Ulivi, 2008; Amin, 2002), while online approaches are less likely to emerge, due to the huge complexity. Among the others, the FP7 MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures) project has achieved promising results by developing a secure online software architecture and by sharing information on a real time basis among local risk predictors, in order to obtain accurate and synchronized predictions using shared interdependency models (Capodieci, Foglietta, Lefevre, Oliva, Panzieri, Delli Priscoli, Castrucci, Suraci, Khadraoui, Aubert, Jiang, Spronska, Diblasi, Ciancamerla, Minichino, Setola, De Porcellinis, Lev, Shneck, Iassinovski, Simoes, Caldeira, Harpes and Aubigny, 2010). The outcome of this process is that operators receive information about the future evolution of their infrastructure with a wider perspective compared to previsions that can be generated by sector specific and isolated simulators.

While MICIE project has proved that increasing cooperation among infrastructures' owners by sharing information leads to better previsions, such an integration is not enough in order to quickly and effectively react to all adverse events that may occur over the System of Systems and, in particular, to face cyber attacks. Cyber attacks against SCADA (Supervisory Control And Data Acquisition) systems are considered extremely dangerous for CI (Critical Infrastructure) operativeness and must be addressed in a specific way. As an example, one of the most adopted attacks to a SCADA system is based on fake commands sent from the SCADA to the RTUs (Remote Terminal Unit).

In order to effectively react to a specific low level menace, there is the need to consider both the global and the local perspectives. In fact, besides obtaining a wider perspective on the state of the System of Systems, there is the need to increase the intelligence of equipment and devices that are used to influence the behaviour of the system, such as RTUs, valves, etc.

The idea to add "intelligence" to the field is not new; electro-valves for gas pipelines are available on the market that, in the case they receive a rapid sequence of open-close commands, do not perform them in order to avoid the consequence of the mechanical shock.

The CockpitCI approach, in order to overcome such catastrophic vision, aims to improve the resilience and the dependability of CIs through the design and the

Proceedings of the International Defense and Homeland Security Simulation Workshop 2012
ISBN 978-88-97999-08-9; Bruzzone, Buck, Longo, Sokolowski and Sottilare Eds.

implementation of an Alerting System that provides to CI operators an efficient tool to support them: (i) in the prevention of cyber attacks, and (ii) in the implementation of consequence containment strategies in case of attack.

In order to reach this goal, at low field level equipment will be provided of some kind of intelligence, allowing them to be able to perform local decisions but only in the presence of "critical" situations, i.e. those characterized by a high risk in terms of on-going cyber attack or unavailability of the communication. This approach will increase both global awareness and local decision-making capability.

2. METHODOLOGY

In the framework of giving "intelligence" to the low-level field equipment, a mandatory element to be considered is the capability of the different actuators (e.g. RTUs) to contrast cyber attacks by identifying them and operating, even in the absence of information coming from the central SCADA, in a "safe" manner. This implies to increase the "intelligence" at RTU level providing them with some form of self-healing and self-protection capabilities. However, it is important to understand that for SCADA systems currently used to monitor and control Critical Infrastructures, it is very dangerous that RTUs can perform autonomous operations or refuse to execute requested commands. To overcome such contradictory behaviour a sort of hybrid schema will be considered and developed in the CockpitCI project:

- at the level of Control Centre, the presence of an "Integrated On-line Risk Predictor" will perform an accurate situation assessment and will provide the operator with a qualitative/quantitative measurements of near future level of risk integrating data coming from the field, data coming from other infrastructures and data coming from smart detection agents monitoring possible cyber attacks.
- at field level, the schema is complemented with a smart software layer for RTUs and a detection system for the TLC (Telecommunication) network. This layer will continuously analyze the inputs and outputs of the RTU in order to prevent misuse, and will analyze the traffic on the TLC network to recognize cyber attacks.

As long as the smart layer does not receive an arming command from the SCADA, it will continue to execute commands received from the SCADA, even if there are large discrepancies between the expected commands and the ones actually received. On the other side, when the RTU is armed (i.e., there is a high risk level), the RTU may eventually neglect the received commands and actuate locally by defined ones. This implies the creation of a local vision of RTUs environment that will continuously evaluate optimal reaction strategies.

With respect to cyber attacks, CockpitCI project aims to improve resilience and dependability of CIs through the design and implementation in each CI of the CockpitCI Integrated Risk Prediction System. The main improvement addresses the detection, prevention and reaction to cyber threats. More specifically, the CockpitCI system will:

- develop and deploy smart detection agents to monitor the potential cyber threats according to the types of ICT based networks (SCADA, IP…) and types of devices that belong to such networks;
- identify, in real time, the CI functionalities impacted by the cyber attacks and assess the degradation of CI delivered services;
- broadcast an alerting message through an improved Secure Mediation Gateway at different security levels (low and high level);
- manage a strategy of containment of the possible consequences of cyber attacks at short, medium and long term.

The above-mentioned cyber threats and the assessment of consequences will be expressed in terms of risk level for a given CI of being no more able of providing its services with its target QoS (Quality of Service) in consequence of events occurring in other CIs; such a risk level will be hereinafter referred to as CI risk level. So, the CockpitCI system will be able to provide, in real time, each CI operator with a CI risk level measuring the possibility that, in the near future, he will no more be able to provide the CI services with the desired QoS in consequence of faults or cyber attacks, and from a high level point of view, the CockpitCI system will be able to provide a map of potential cyber threats on CI network.

The CockpitCI system will analyze in real time the cyber threats according to adaptive algorithms, compute the CI risk on the basis of abstract CI models (forecasting CI QoS taking indicators, accounting mutual interdependency among CIs and cyber attacks) and on a suitable set of aggregated data from raw field data, collected in real time by means of adequate interfaces.

3. DEVELOPMENT

The CockpitCI approach is based on the following concepts, models, equipment and tools:

(1) QoS prediction models. Quality of Service prediction models have the final aim of predicting the QoS delivered by interconnected SCADA and Telco networks accounting for cyber vulnerabilities and cyber attacks. The models will predict indicators of QoS delivered by the interconnected networks by adequate representation of the technological networks, their cyber vulnerabilities and adverse events, including cyber attacks (Bobbio, Bonanni, Ciancamerla, Clemente, Iacomini, Minichino, Scarlatti, Terruggia and Zendri, 2010; Bobbio, Ciancamerla, Diblasi, Iacomini, Mari, Melatti, Minichino, Scarlatti, Terruggia, Tronci and Zendri, 2009; Ciancamerla, Foglietta, Lefevre, Minichino, Lev andShneck, 2010; Ciancamerla, Di Blasi, Foglietta, Lefevre, Minichino, LevandShneck, 2010). The activity will be fed by an overview of modeling techniques and tools for cyber threats and

cyber vulnerabilities analysis of interconnected of SCADA systems and Telco Networks and SCADA systems. Prediction models will predict the attributes of readiness, reliability, security and performances of such services. Models will be built according to heterogeneous paradigms selected according to their capacity to represent the impact of adverse events (cyber threats, internal failures, network congestions and natural phenomena) on the QoS delivered by SCADA and the interconnected Telco networks. Modeling paradigms will include adequate agent based simulation, analytical dependability modeling with careful examination of scalability issues (Extended Stochastic Petri Nets, Network Reliability analyzers) discrete event simulation (based on largely known open source platforms) and Input/output modeling.

(2) The design and the implementation of the CockpitCI Detection System (detection agents plus detection adaptors). This part will include research aspects (especially in terms of smart detection agents for SCADA and Telecom network) and integration aspects (taking into account existing system). Especially, this concept will include the research aspects on traffic monitoring and attack detection, i.e. new machine learning based approaches for unusual traffic event detection will be investigated. At the end of this phase, the different approaches will be evaluated and the most suitable solution for cyber attack detection will be selected. The final objective is to design and implement a set of intelligent detection agents able to identify the cyber threats. These agents will be included in a smart architecture able to be re-oriented thanks to learning strategies.

(3) The On-Line Integrated Risk Predictor (IRP) which, on one hand, will allow to model the cyber-dependencies of CIs and the other functional dependencies, and, on the other hand, will permit to identify the potential cascading effects of cyber attacks or other adverse events using the right interdependency schemes provided by the modeling. The on-line IRP will also implement an accurate situation assessment to devise best responses to the actual threat and identify the part of risked CI network, and to broadcast relevant information to other CI and national/European authorities.

(4) The design and implementation of the CockpitCI Secure Mediation Network in the prospect of broadcasting cascade failures and cyber alerts at low and high level.

(5) The design of a CockpitCI Smart RTU Reaction System which, on the grounds of the CockpitCI On-Line Risk Predictor, will manage the strategy of containment, i.e.: (1) to block attacks, (2) to isolate infected systems, (3) to deploy tactical and operational security policies.

(6) The design and implementation of the CockpitCI SCADA adaptors to extract raw data from SCADA and Telco control rooms but also from other SCADA and Telco devices (Smart RTUs, Detection Agents, etc.)

In particular, the methodology in question will be based on the following issues:

a. To identify a typology of cyber-threats and to model the cyber-interdependencies of the composite CIs system in order to identify the right peers to communicate alert messages for each type of cyber-attacks.

b. Develop a real-time Distributed Monitoring System and Perimeter Intrusion Detection System (PIDS) able to aggregate the filtered and analyzed information of potential cyber-attacks induced on SCADA systems or telecommunication systems used to support the operation of CIs and identify the potential unsecured area of the CIs. Thanks to intelligent detection agents, the monitoring system should be able to dynamically reconfigure itself in order to focus on specific threats.

c. Create a framework to allow the community of CI owners to exchange real-time information about attacks (and tentative attacks), extending the capabilities and functionalities of the Secure Mediation Gateway and of the risk prediction tool developed in MICIE project. Issues to be considered include: (i) need to exchange information among trusted CIs, not necessarily interdependent, (ii) availability of the integrated prediction tool in each CI to calculate cascading events induced by faults and cyber attacks especially in terms of QoS of Power and Telecommunication Grid, (iii) need to develop a strategic analysis tool able to calculate the potential threat of coordinated cyber-attacks on CIs.

d. Analyze strategies for automatic real-time reaction able to better manage the corrupted portion of the grids (Telco and SCADA), able to predict the time of reconfiguring the grid to reach a defined QoS level, and able to treat the corrupted system at short, medium and long term (definition of automatic procedures of treatment).

Another fundamental aspect addressed by the CockpitCI approach is the secure exchange of information across CIs and to high level authorities (national or European). The CockpitCI system, based on Secure Mediation Gateways, will be capable to allow secure broadcasting of the information at low and high level. The use of the new Secure Mediation Network will assure that information sharing regarding CI is mediated and elaborated to support decisions and, at the same time, it takes place in an environment of trust and security. The sharing of information requires a relationship of trust such that companies and organizations know that their sensitive data are sufficiently protected.

The CockpitCI system, including detection, prediction, alert and reaction, will be conducted by means of a reference scenario. Reference scenario identifies the portion of the interconnected SCADA system and Telco network, selects services delivered to customers, evaluates their quality (in terms of continuity, readiness, performances, time response), finds the vulnerabilities in the interconnected networks for possible cyber attacks and cyber interdependencies between networks in order to mitigate the effects of successful cyber attacks. A reference scenario is in an operational mode when the quality of the delivered services (QoS) is within a Service Level Agreement (SLA), or in a degraded mode when QoS is outside SLA as an ultimate consequence of successful cyber attacks or other adverse events.

4. PRELIMINARY RESULTS AND CONCLUSION

The accomplishment of the proposed objectives will bring noteworthy added value to specific application scenarios. In the following, the ideas, concepts and objectives presented in the previous sections have led to the definition of the following architecture of the CockpitCI system. The envisaged CockpitCI system architecture, in the case where two interdependent CIs are considered, is shown in Figure 1.

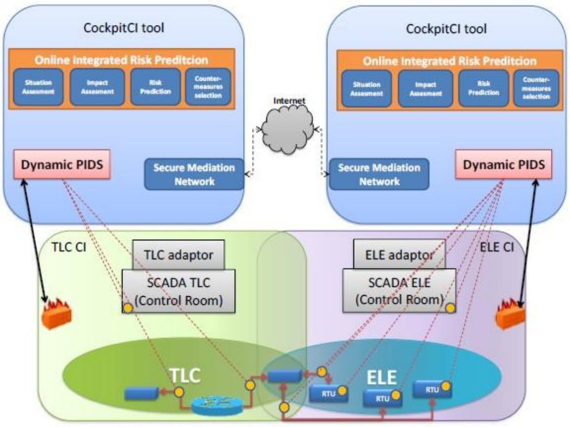


Figure 1: Envisaged CockpitCI architecture.

At the bottom of the figure, a conceptual and simplified illustration of the two CIs and of their interconnection is presented. In particular, for the sake of exposition, a telecommunication CI ("TLC" in the figure) and an electric distribution network ("ELE" in the figure) are considered. For each CI, both field elements (e.g. RTUs) and the SCADA control room ("SCADA ELE" and "SCADA TLC") are represented (the CockpitCI tool interacts both with field level devices and at control room level). Each CI has an associated CockpitCI tool. Since the CockpitCI tool must be a scalable and CI-technology independent solution, it is necessary to consider in the architecture also proper adaptors ("TLC adaptor" and "ELE adaptor" in the figure) at the interface between the CockpitCI tool and the particular CI domain. The CockpitCI tool architecture consists of three layers, namely detection layer, risk prediction layer and mediation layer.

As concerns the components lying at detection layer, they consist of (i) a centralized component, named dynamic PIDS (Perimeter Intrusion Detection System), and (ii) a set of distributed local detection agents for intrusion detection at local level (the yellow dots in the figure). The local detection agents will be able to autonomously detect and (in some cases) react to local attacks, and will provide information to distributed Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) mechanisms. Detection agents, adaptors and extensions for system components will pervade CI's field and will be placed at the most critical sources of vulnerabilities, including RTUs and the main SCADA elements. The PIDS is a centralized component which correlates and aggregates the alerts received from the detection agents. Moreover, the PIDS has the capability to detect coordinated cyber-attacks, and to dynamically deploy containment or even preventive strategies of isolation (as an example, the PIDS could respond to detected threats by changing firewalls rules in order to redefine ICT system perimeters).

Information from local detection agents is gathered by adaptors (which perform all the needed operations in terms of filtering, aggregation, translation, etc.), and sent (in a technology independent format) to a centralized on line Integrated Risk Prediction (IRP) (at the top of the figure), which performs a situation assessment, computing the risk level associated to the current state of the CI, and evaluates the impact of cyber-attacks, suggesting also possible countermeasures. The IRP performs the above-mentioned situation assessment by properly analyzing rich input information merging both local field information (coming from the local CI Detection Layer) and global/remote information about the status of linked CIs, coming from linked IRPs. Notably, the connection between the IRP and the local detection layer is bidirectional in the sense that the results of IRP elaborations can be fed-back to the detection layer (to local detection agents and PIDS) in order to improve local detection and reaction capabilities. Hence, the output of the IRP will be provided both to control room operators and to the detection layer.

The secure and reliable communication between the detection layer and the IRP is assured by a secure mediation network, which also supports the secure exchange of data between linked CIs. So doing, it is possible to combine local and global perspectives and obtain awareness at all the levels of the system. This is essential in view of the concept of interdependence, which plays a crucial role in critical infrastructures protection. Concluding, the proposed CockpitCI architecture is functional to the achievement of the general objectives explained in the previous sections, which impose innovative technological and scientific contributions in the fields of CI modeling, cyber detection, risk prediction, adaptors design, secure mediation of data and intelligence for local autonomous reaction capabilities.

REFERENCES

Amin M., 2002. Modelling and Control of Complex Interactive Networks. *IEEE Control System Magazine*, pp. 22–27.

Bobbio A., Bonanni G., Ciancamerla E., Clemente R., Iacomini A., Minichino M., Scarlatti A., Terruggia R., Zendri E., 2010. Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network. *Reliability Engineering and System Safety Journal, Elsevier editor*.

Bobbio A., Ciancamerla E., Diblasi S., Iacomini A., Mari F., Melatti I., Minichino M., Scarlatti A., Terruggia R., Tronci E., Zendri E., 2009. Risk analysis via heterogeneous models of SCADA interconnecting Power Grids and Telco Networks. *CRiSIS'2009 – The Fourth International Conference on Risks and Security of Internet and Systems*, 19-22 October 2009, Toulouse, France.

Capodieci P., Foglietta C., Lefevre D., Oliva G., Panzieri S., Delli Priscoli F., Castrucci M., Suraci V., Khadraoui D., Aubert J., Jiang J., Spronska A., Diblasi S., Ciancamerla E., Minichino M., Setola R., De Porcellinis S., Lev L., Shneck Y., Iassinovski S., Simoes P., Caldeira F., Harpes C., Aubigny M., 2010. Improving Resilience of Interdependent Critical Infrastructures via an On-Line Alerting System.*Proceedings of COMPENG 2010 - Complexity in Engineering*.

Ciancamerla E., Di Blasi S., Foglietta C., Lefevre D., Minichino M., Lev L. Shneck Y., 2010. QoS of a SCADA system versus QoS of a Power distribution grid. *10th International Probabilistic Safety Assessment & Management (PSAM)*. June 7-11, 2010, Seattle, WA.

Ciancamerla E., Foglietta C., Lefevre D., Minichino M., Lev L., Shneck Y., 2010. Discrete event simulation of QoS of a SCADA system interconnecting a Power grid and a Telco network. *1st IFIP International Conference on Critical Information Infrastructure Protection, World Computer Congress 2010*. 20-23 September 2010, Brisbane, Australia.

De Porcellinis S., Panzieri S., Setola R., Ulivi G., 2008. Simulation of Heterogeneous and Interdependent Critical Infrastructures. *International Journal Critical Infrastructures (IJCIS)* Vol. 4, n. 1/2:pp. 110-128.

Haimes Y., Horowitz B., Lambert J., Santos J., Lian C., Crowther K., 2005. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. *Theory and Methodology, Journal of Infrastructure Systems* Vol. 11(2):pp. 67-79.

Suter, M., Brunner, E.,2008. International CIIP Handbook 2008/2009. *Centre for Security Studies,* ETH Zurich.

AUTHORS BIOGRAPHY

Donato Macone, Ph.D student in the Department of Information, Electrical and Telecommunication Engineering (DIET) of “Sapienza” University of Rome. He graduated with Bachelor Degree in Computer Engineering in 2007 with 110/110 cum laude and graduated with Master Degree in Computer Engineering in 2009 with 110/110. His expertise covers network resource management, game theory, ontology representation, routing and load balancing strategies and algorithms, algorithms for data fusion. He participated in the MICIE project, fund within the FP7 EU ICT-SEC research programme and is still involved in TASS and CockpitCI projects, fund within FP7 EU SEC research programme, SMARTV2G project, fund within the FP7 EU ICT-GC research programme.

Francesco Liberati received the bachelor degree and master degree in automatic control engineering and systems engineering from "La Sapienza" University, Rome, Italy, in 2009 and 2011, respectively. He is currently working toward the Ph.D. degree in systems engineering at the same university. His research interests include critical infrastructures protection and the application of control systems theory to the design of local energy management systems, with applications to smart grids and electromobility.

Andrea Simeoni, Master degree in Computer Engineering, achieved in "La Sapienza" University of Rome. His research activity covers resource management and routing algorithms for future networks, cross platform development frameworks, Software Defined Networking and critical infrastructure security.

Francesco Delli Priscoli is Full Professor at the University of Rome "La Sapienza" where he holds the courses "Automatic Controls", "System Control" and "Network Control and Management I and II", and is a member of the board of directors of CRAT. His main research topics are nonlinear control and QoS/resource management procedures for mobile systems. He is the author of about 160 papers and four patents. He was/is presently responsible, at the University of Rome "La Sapienza", for 18 projects financed by the EU or by ESA dealing with resource management, service and interworking management for broadband terrestrial and satellite wireless/wired systems.

Marco Castrucci graduated in Telecommunication Engineering with 110/110 cum laude in May 2006 at the University of Rome “La Sapienza” and obtained the Ph.D. in System Engineering from University of Rome “Sapienza” in 2010. He was involved in FP6 IST ‘DAIDALOS II’ and ‘WEIRD’ projects and FP7 ICT 'OMEGA', 'MICIE', ‘FI-WARE’ and ‘MONET’ projects. He also covered WP leader position in several of the mentioned projects. His main research topics were related to the convergence among heterogeneous telecommunication technologies, the design of innovative architectures and paradigms for the Internet of the Future, and software defined networks. He is author of several publications related to its research activities. At the moment he works for Business Integration Partners, as business consultant in the public sector.

Stefano Panzieri (http://panzieri.dia.uniroma3.it) was born in Rome (Italy) on December 17th 1963. He took the Ph.D. in System Engineering in 1994 at University of Rome “La Sapienza”. From 1996 he is with the University “Roma Tre” as Associate Professor. His teachings are in the field of Automatic Control, Digital Control and Process Control within the courses of Electronic, Mechanics and Computer Science, he is the coordinator of both “Automatic Laboratory” and “Robotics and Sensor Fusion Laboratory” ofDip. Informatica e Automazione. He is IEEE member and has been a member of the Working group on Critical Infrastructures of Prime Minister Council. Research interests are in the field of industrial control systems, robotics, sensor fusion and critical infrastructure protection (CIP). In the CIP field has contributed to develop a simulation model, the CISIA project, that is able to evaluate cascades of failures in a network of infrastructures, pointing out hidden interdependencies. Several published papers, in the robotics field, concern the study of iterative learning control applied to robots with elastic elements and to nonholonomic systems. In the area of mobile robots, some attention has been given to the problem of navigation in structured and unstructured environments with a special care to the problem of sensor based navigation and sensor fusion. Many techniques derived from Fuzzy Logic, Bayesian Estimation (KalmanFilltering) and Dempster-Shafer theory have been developed and applied to the problem of mapping building and vision based localisation. More recently, has been interested to the application of complex networks theory into evolutionary computation. He is author of about 100 papers, among them several experimental papers involving mobile and industrial robots.

Serguei I. Iassinovski. Graduated from Moscow Bauman State Technical University in 1985, Ph.D in applied sciences (1990), project manager and team leader at Multitel since 2007. Author of more than 70 publications in the fields of complex discrete system modelling, simulation, optimisation and real-time control, using of AI methods for complex discrete system simulation tools, Business Process Re-engineering, meta-heuristics, scheduling

Michele Minichino received his in Electronic Engineering, “summa cum laude” from University of Naples in 1978. He is coordinator of the program for Critical Infrastructure Protection (CIP) at ENEA. His research interests include risk based methodologies, qualitative and quantitative indicators, multi formalism and multi solution methods and tools for Quality of Service measures (in terms of performances, reliability and dependability) of Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and of large interconnected CI, including power grids and telco networks at regional/national level. He has acted in the frame of several research programs, funded by Italian government and by European Union; among the most recent SHIP, ISAEUNET, SAFETUNNEL and IRRIIS EU Projects. He has been Contract Professor, at the Software Engineering Chair of the Engineering Faculty of the II University of Rome "Torvergata", for several years. He has been Contract Professor of Mainframe Operating Systems, at the High School of the Italian Ministry of Finance (ScuolaEzioVanoni). Currently, he is working on scenarios, services, heterogeneous models and tools to assist on line the operators of ICS and CI in performing emergency procedures, in the framework MICIE (Tool for systemic risk analysis and secure mediation of data across Critical Infrastructures) and CockpitCI (Cyber security on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures) EU FP7 Projects. He serves, as expert, the EU Directorate General Information Society and Media (DG INFSO) and the European Network and Information Security Agency (ENISA) on the topics of the security and resilience of ICS for CIP. He has authored and co-authored more than 70 papers for International Journals and Conferences Proceedings.

Ester Ciancamerla received her degree in Nuclear Engineering from University of Rome on 1978. Since her degree, she has been working at ENEA, as scholarship holder and researcher. In remote past, major experience has been gained dealing with system validation, software verification plans, software test methodologies, tools and environments for computer based systems in nuclear, avionics and railway fields. Her current research interest is on modeling methods and tools for dependability/survivability evaluation of networked systems. She has acted in the frame of several research programs, funded by Italian research organizations and by European Union; among the most recent SHIP, ISAEUNET, SAFETUNNEL and IRRIIS EU Projects. In SAFETUNNEL IST Project, she worked on the validation by modeling of a Tele Control System, based on a Public Mobile Network, for Alpine Road Tunnels protection. She has worked on IRRIIS (Integrated Risk Reduction of Information based Infrastructure Systems) IP – EU project, funded by FP6, to investigate risk based methodologies for vulnerability and interdependency analysis of critical infrastructures. Currently, she is working on scenarios, services, heterogeneous models and tools to assist on line the operators of the interconnected power grid and Telco network in performing emergency procedures, in the framework MICIE (Tool for systemic risk analysis and secure mediation of data across Critical Infrastructures) and CockpitCI (Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures) EU FP7 Projects. She has authored and co-authored more than 70 papers for International Journals and Conferences Proceedings.

HEURISTIC APPROACH FOR PATHS' COMPUTING OF A MARINE FLEET FOR AN UNDERWATER PATROLLING MISSION

D. Balestrieri [a], G. Vaccaro [b], F. Lancia[b] , F. Portieri[a]

[a] INTECS S.p.A. – Traffic Control Division - Salita del Poggio Laurentino 7 – 00144 Roma (Italy) - www.intecs.it
[b] Università degli Studi Roma Tre – Dipartimento di Informatica e Automazione – Via della Vasca Navale 79 – 00146 – Roma (Italy) - www.dia.uniroma3.it

[a]domenico.balestrieri@intecs.it, [b] giu.vaccaro@stud.uniroma3.it, [c] fra.lancia@stud.uniroma3.it,
[d]fabio.portieri@intecs.it

ABSTRACT

Nowadays, the hypothesis of using low cost "unmanned" vehicles, to replace men into territorial waters' surveillance operations, is taking over. This would allow few operators to patrol great sea areas, reducing consequently costs of patrolling missions led by human resources. Because of low autonomy of robotic vehicles, compared with the autonomy of normal vehicles, path's planning algorithms are needed to maximize the length of each path, respecting each vehicle's autonomy and the constraints due to the vehicles' features, revisits of sensible areas etc. etc. The following article describes a heuristic approach to the computing of these navigation plans.

Keywords: patrolling, optimization problem, path planning, submarine vehicles.

1. INTRODUCTION

The main activities carried out by the Coast Guard, are focused on improving the sailing security, the protection of the marine environment and ensuring the respect of National and International laws. For this purpose, a great number of resources are involved in daily coast patrolling operations, with consequently high costs. To reduce these costs, joint missions with other police teams are carried out. This is not always enough to ensure sufficient surveillance, due to, for example, a great number of coast's Kilometers (e.g. Italy has more than 8000 km of coasts). The risk is to leave some areas "unvisited", which might be particularly sensible, for which the maritime safety and/or the marine environment could be compromised. This article is focused on the problem of a submarine patrolling, or else the problem of patrolling sea sub-areas located at different depths. This is an important matter for what concerns the protection of marine environments and the improvement of the sea security.

Using "unmanned" vehicles to support patrolling operations would allow surveillance of great sea extensions with very few operators, allowing the local government, employed into monitoring of its territorial waters, to exploit in an efficient way its own resources of men and vehicles.

2. THE PATROLLING PROBLEM

2.1. A submarine sea area's patrolling

The problem of a submarine sea area's patrolling can be defined as follows: *"given a set of vehicles and an area, the paths assigned to each vehicle must be calculated taking into account that each point into the area would be visited by at least a vehicle"*.

Consequently, the following hypothesis can be formulated:

1. *Sailing autonomy*: each vehicle has its own sailing autonomy, which is the capacity of patrolling a certain amount of miles, depending on its fuel.
2. *Area points*: visiting some area points could be seen as visiting some interesting sites, such as buoys or strategic points, or else, given a precise sea area, visiting it all. We assume that vehicles have a 360 degrees sight of a certain ray, depending by the sensor installed on each vehicle.
3. *Sea Strength*: a point's sea strength is represented by an integer number between 0 and 9 which gives and information about the sea state into that area, based upon the Beaufort scale (i.e. 0=calm, 9=windstorm). Each vehicle has a certain sea capacity, defined by an integer number between 0 and 9 as well, that indicates the maximum sea strength that the hull can endure (i.e. a vehicle with sea capacity C can visit a point having sea strength F if $C \geq F$).
4. *Equipment*: each vehicle is equipped with particular tools and/or sensors. Some points of the area may require vehicles equipped with a certain tool (for example, it may be a weapon).
5. *Revisiting sensitive points*: some points of the area may be considered more "sensitive" than others, so that they require a revisit, for example at defined time intervals, by at least a vehicle.
6. *Obstacles presence*: some points might not be patrolled because of the presence of "obstacles" (i.e. islands, low backdrops, etc. etc...)
7. *Depth:* each vehicle can travel at different depths, considering its own depth constraint. Each node of the sea selected area is located at a different depth.

The optimization problem of the patrolling of a submarine sea area consists in searching for a “better” solution, composed by a set of paths, in order to visit the selected sea area fully, with the minimum time and considering the hypothesis above.

It’s important to underline that the “best” solution (a more “efficient” patrolling) may involve only some available vehicles.

3. THE PATROLLING PROBLEM SEEN AS A MTSP

3.1. Variants to the original problem

Solution of the patrolling problem can be reconducted to the well-known mTSP in literature (multiple Travelling Salesman Problem) (see Brummit and Stentz (1996), Brummit and Stentz (1998), Yu et al. (2002), Ryan et al. (1998). The mTSP consists of a generalization of the Travelling Salesman Problem with more than one salesman (see Mole et al. (1983), Laporte et al. (1985), Toth and Vigo (2002)).

The classic mTSP formulation provides that the m salesmen must visit each city only one time, with the minimum possible “cost”.

In the specific case of the patrolling problem, the following variants to the original formulation must be considered:

- *Multiple Deposits*: more deposits exist, with a certain number of salesmen dislocated into each of them. The salesmen can return into their own starting deposit after completing the tour or return into a random deposit (the initial number of salesmen must remain the same at the end of the trip).
- *Number of salesmen*: the number of salesmen can be represented by a limited variable or can be a fixed number.
- *Fixed cost*: if the number of salesmen isn’t fixed, then each salesman has usually a fixed cost attributed, which has to be added to the function cost whenever this salesman is employed into the solution.
- *Time Windows*: some points must be visited into determined time intervals, named *time windows*. This is an important mTSP extension and it’s named as Multiple Travelling Salesman Problem with Time Windows (mTSPTW) (see Macharis and Bontekoning (2004), Wang and Regan (2002), Ruland and Rodin (1997), Mitrovi´et al. (2004)).
- *Other restrictions*: these restrictions consist in a particular constraint on a particular equipment of the vehicle (salesman), which visits a point, on the vehicle’s capacity to sustain sea’s strength in that point, on the maximum length of paths attributed to each single vehicle, due to their autonomy and on the presences of obstacles.

4. PROBLEM DEFINITION

Given :

- A graph $G = (V,E)$ where V is a set of vertexes and E a set of arcs with a specific “cost” connecting vertexes;
- m, the number of salesmen (vehicles);
- deposits $D_i \in G$ from which salesmen must start their trip;
- $\mathbb{X}$ set of all possible configurations, or all possible choices of m paths starting from and ending into the assigned deposit and visiting once and only once each one of all the other vertexes;
- $\boldsymbol{v}$ set of constraints;
- $\mathbb{X}_{\boldsymbol{v}}$ sub-set of the configurations respecting the assigned constraints $\boldsymbol{v}$;
- $f : x \in \mathbb{X} \mapsto \mathbb{R}$ cost function assigned to the problem solution.

Solving the patrolling problem consists in finding a configuration x□ $\in \mathbb{X}$ which respects the constraints and minimizes the total cost, or: x=min(f(x)) with $x \in \mathbb{X}_{\boldsymbol{v}}$.

4.1. Graph construction

The set V of graph’s vertexes is built by coverage of the free-space by a Voronoi diagram. Cells of the diagram have a maximum ray compatible with the sensibility of the sensor used for patrolling, installed on each vehicle.

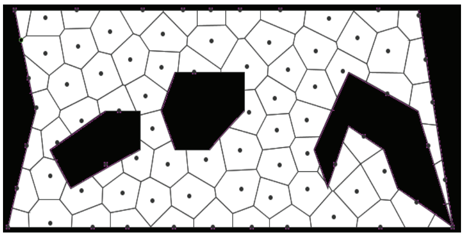


Figure 1: Voronoi Diagram

Vehicles and areas that have to be visited are considered as points while the obstacles are modeled as polygons, defined by their vertexes.

The set *E* is composed by all arcs of a complete graph built with the *V* set of vertexes, where each arc of the graph has an associated cost, equal to the Euclidean distance of its vertices, considering their latitude, longitude and depth.

4.2. Cost function

The cost function $f : \mathcal{X} \mapsto \mathbb{R}$ is defined on the set $\mathcal{X}$ of all possible solutions and is computed as:

$$f(x) = \sum_{p \in \{\text{paths of solution } x\}} [length\ (p) + penalty(p)]$$

with:

- *length (p)* = length of the path *p* (assigned to a vehicle) and belonging to the solution *x*
- *penalty(p)* = sum of all penalties of path *p*

penalties are computed as follows:

- *Penalty for vehicle's autonomy*

Autonomy is the maximum length of a path that a vehicle could make. The penalty for a path's autonomy *p* is:

$$penalty(p) = FMULT \cdot [c(p) - cmax(p)]$$

with:

- *c(p)* = length of path *p*
- *cmax(p)* = maximum length of *p*
- *FMULT* = empirical multiplicative factor

The algorithm will try to satisfy the constraint considering high values of *FMULT* constant. But a too high value of *FMULT* may cause the algorithm to stop into a cost function's local minima.

- *Penalty for time windows*

Revisiting of one or more vehicles on a site is equivalent to define time windows (more or less regular) on this site, which at least a vehicle must visit. Time windows are attributed each one to a different node with the same position, added to the set *V* of graph *G* (i.e. if a node has to be visited twice, there could be added to the map other two nodes into the same position, but having different time windows). If a vertex *v* belonging to a path *p* is associated to a time window [$t1_v$, $t2_v$] (with $t1_v$, $t2_v$ minimum and maximum visit time), and the visit time on that node, following *p*, is *t(v)*, the related penalty is computed as:

$$penalty(p) = TMULT \cdot [\sum_{v \in p} windowPenalty(v,t1_v,t2_v)^2]$$

with:

$windowPenalty\ (v,t1_v,t2_v) = 0 \ \ se\ \ t1_v \le t(v) \le t2_v$

$windowPenalty\ (v,t1_v,t2_v) = t(v) - t2_v\ se\ t(v) > t2_v$

$windowPenalty\ (v,t1_v,t2_v) = t1_v - t(v)\ se\ t(v) < t1_v$

and *TMULT* empirical multiplicative factor.

- *Sea Strength Penalty*

Sea strength on a vertex *v* is defined as an integer number *s(v)* between 0 and 9, and each vehicle *m* sustain a maximum sea strength *s(m)*. A vehicle having strength *s(m)* can visit a site with strength *s(v)* if *s(m) ≥ s(v)*.

Sea strength penalty of a path *p* is:

penalty(p)=MMULT · (#nodes v s.a. s(v)> s(m))

with *MMULT* empirical multiplicative factor.

- *Equipment Penalty*

Some nodes might have the constraint that they could be visited only by vehicles equipped with a particular sensor or tool (or weapon).

The equipment penalty of a vehicle with a path *p* is computed as follows:

penalty(p)=EMULT · (#nodes v s.a. m isn't provided with the right equipment required by v)

With *EMULT* empirical multiplicative factor.

- *Penalty for long arcs*

To avoid inserting long arcs into the final solution, optimizing the length of each sub-path, a possible choice is to associate a penalty if the distance between two connected nodes into a path *p* is longer than a certain length *l,* as *2*ray of the sensors* equipped on each vehicle.

The penalty for long arcs is as follows:

penalty(p)=LMULT· (#arcs e associated to vehicle m *s.a. l(e) > 2*ray of the sensors* equipped on m*).*

With *LMULT* empirical multiplicative factor.

- *Obstacles Penalty*

A vehicle must necessarily avoid obstacles into the sea area that needs patrolling: this has been made inserting a certain penalty in case at least one of the arcs belonging to the set of paths would go through one of the obstacle's sides.

The obstacles penalty is computed as*:*

penalty(p)=OMULT if at least an arc belonging to the set of paths P goes through one of the obstacle's sides.

With *OMULT* empirical multiplicative factor.

5. HEURISTIC APPROACH

The heuristic approach used to solve the patrolling problem is the Simulated Annealing.
This algorithm is also called "meta-heuristic" and consists into an extension of the classical local search.
Considering the local search, when a solution's neighborhood is explored, the only information owned is the best current solution and the related cost function value.

5.1. Simulated Annealing

This approach, used to solve the patrolling problem, is inspired by the industrial process named annealing, and it's known in literature with the name of *Simulated Annealing* (see Aarts and Korst (1989), Dekkers and Aarts (1991), Romeijn and Smith (1994)). While a liquid's molecules tend to move freely at high temperatures, if a temperature is lowered in a sufficiently slow way, the molecules' thermic mobility is lost and they tend to form a pure crystal corresponding to a minimum energy state.

The annealing is a thermic treatment used mostly on steel and copper, the slower cooling we have, the stabler structure we obtain. Similarly, the approach tends to converge to an optimal solution (see Bélisl (1992), Locatelli (1996), Locatelli (2000)) using this heuristic and choosing a decreasing sequence of temperatures, with a sufficiently slow 'cooling': as we arrive to a minimum energy state through the physical process, in the same way we obtain a solution (the global optima) with a minimum cost function value, using the annealing into optimization problems.

The peculiarity of Simulated Annealing is the capacity to avoid local minima accepting also the transitions that increase the value of cost function f. Accepting configurations with a worse cost function is the only way to escape from local minima.

The heuristic is articulated into the following steps:

1. A sequence of temperatures $T_0>T_1>T_2>$... with T_i tending to 0 for $i \rightarrow \infty$ is fixed;
2. A rounded positive numbers sequence $N_0>N_1>N_2>$... and an iterator $j = 0$ are fixed;
3. The initial solution is generated;
4. $T = T_j$ and $N = N_j$, and an iterator $i = 0$ are set;
5. If $i <= N$ go to Step 6., otherwise go to Step 9.
6. A new random solution *x'* is generated (see par. 5.2)
7. If $f(x') < f(x)$ then $x = x'$, otherwise $x = x'$ with a certain probability:

$$p = e^{-[f(x') - f(x)] / T}$$

8. $i = i + 1$ and the heuristic returns to Step 5.
9. $j = j + 1$ and the heuristic returns to Step 4.

5.2. Random generation of a solution

To generate a solution randomly, the idea is to start from the last solution and choose randomly one of its "transformations" listed below:

1. Move 1-0 (Relocate)
2. Move 1-1
3. Move 2-0 (Double relocate)
4. Move 2-1
5. Move Or-Opt
6. Move CROSS
7. Move 2-Opt

Once a transformation to apply is found (*Move*), the vehicle containing the first vertex used for the exchange is chosen randomly. The other vertex (or others) involved into the exchange are chosen into the 'neighborhood' of the first vertex.

The different transformations used by the algorithm are:

1. *Move 1-0 (Relocate):* a vertex is moved into another position of the same vehicle's path, or else into another vehicle's path;

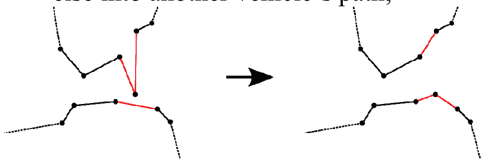


Figure 2: illustration of a "relocate" move

2. *Move 1-1:* a vertex into a vehicle's path is exchanged with a vertex contained into another vehicle's path;

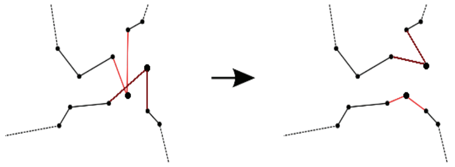


Figure 3: illustration of a move 1-1

3. *Move 2-0 (Double relocate*): a couple of near vertexes is moved into another position of the same vehicle's path or into another vehicle's path;

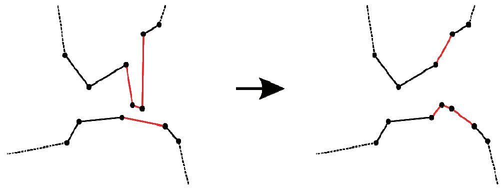


Figure 4: illustration of a "double relocate" move

4. *Move 2-1*: a couple of near vertexes is exchanged with a vertex contained into another vehicle's path;

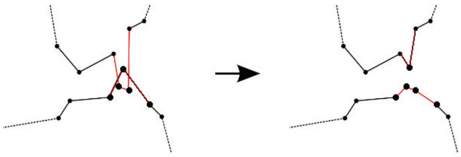


Figure 5: illustration of a move 2-1

5. *Move OrOpt:* two vertexes belonging to the same path swap their neighbors, maintaining all the rest unaltered;

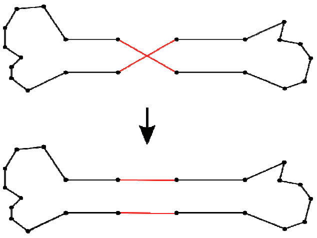


Figure 6: illustration of a move OrOpt

6. *Move CROSS:* two salesmen exchange a sub-path. This kind of move contains also the relocate ones and the exchanges between nodes of different paths (Move 1-1 and 2-1).

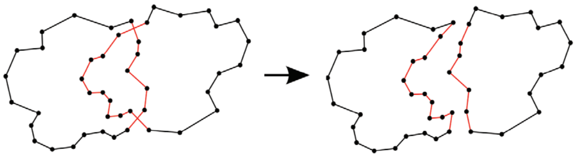


Figure 7: illustration of a move CROSS

7. *Move 2-Opt:* Two vehicles exchange their paths, starting from two vertexes. Two arcs get removed (i.e. *(i, j)* and *(h, k)*) and two new arcs are added, *(i, k)* and *(h, j)*. This is possible if and only if the two vehicles involved end their routes into the same deposit.

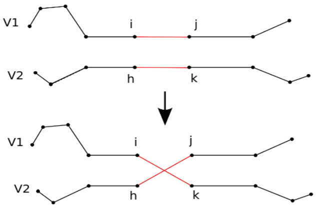


Figure 8: illustration of the move 2-Opt

6. EXPRIMENTAL RESULTS

Here below are shown some results taken from the application of this algorithm, using vehicles having the same maximum velocity but with different autonomy.

Each point of the area is defined by three coordinates:

- x = longitude
- y = latitude
- z = depth

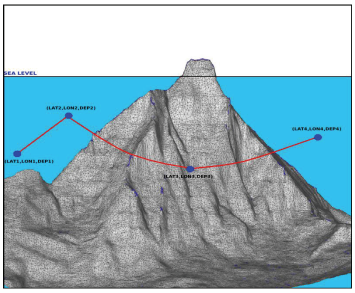


Figure 9: 3D representation of a path

The following cases have been considered:

1. case without any particular point into the sea area (so no particular constraints on sea strength, vehicle's equipment, nor revisits of sensible points)

2. case with all the constraints listed before.

6.1. Case without constraints

In *Figure 10* we may observe paths attributed to each vehicle into the selected submarine sea area: each *path* is represented by a set of arcs colored differently, each *node* is colored in grey, except for the *deposits*, each one having the same color of the path that starts from there. In this example, each node is located at a different depth.

Figure 10: Case without constraints 2D

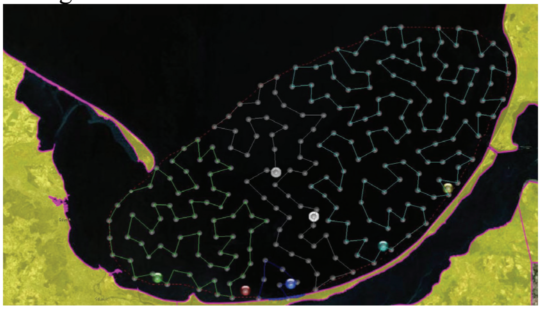


Figure 11: Case without constraints 3D

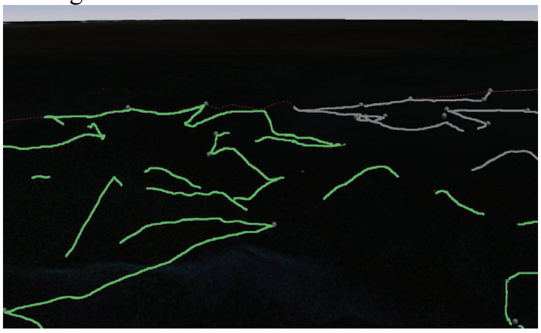


Table 1: Results without constraints

Vehicle	Used	Color	Autonomy (Km)	Vel. (Km/h)	Path Length (Km)
1	YES	RED	233,81	10	0,28
2	YES	BLUE	306,05	10	28,9
3	YES	CYAN	493,55	10	437,71
4	NO	YELLOW	86,91	10	0
5	NO	WHITE	166,3	10	0
6	YES	GREY	497,33	10	176,5
7	YES	GREEN	281,19	10	230,04

Total number of vehicles: 7

Vehicles involved: 5

Solution cost: 873.42Km

It's noticeable that the selected sea area is completely visited using only 5 among the 7 vehicles available.

6.2. Case with constraints

In Figure 11 we may observe paths attributed to each vehicle available into the selected submarine sea area, considering all the set of constraints described before: *nodes* without any particular constraint are represented in grey, nodes with *revisits* are colored in green, the ones with a certain *sea strength* are colored in red, while the ones needing a particular *equipment* are represented in yellow. In this example, each node is located at a different depth.

Figure 12: Case with constraints 2D

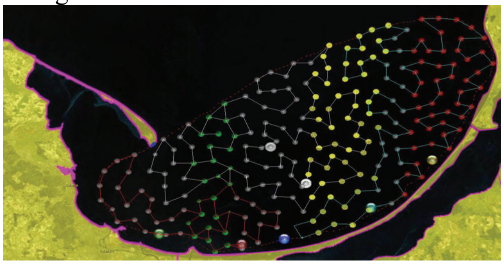


Figure 14: Case with constraints 3D

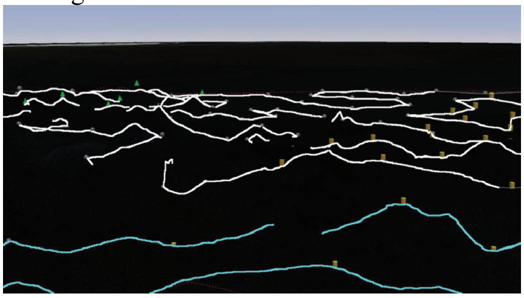


Table 2: Results with constraints

Vehicle	Used	Color	Autonomy (Km)	Vel. (Km/h)	Sea Strength	Equip.	Path Length (Km)
1	YES	RED	430	10	NO	NO	201,15
2	YES	BLUE	449,8	10	NO	YES	3,85
3	YES	CYAN	431,25	10	YES	YES	347,68
4	YES	YELLOW	176,43	10	YES	NO	0,34
5	YES	WHITE	467,92	10	NO	YES	407,15
6	NO	GREY	376,05	10	NO	YES	0
7	NO	GREEN	318	10	NO	NO	0

Total number of vehicles: 7

Vehicles involved: 5

Solution cost: 960.19Km

It's noticeable that the selected sea area is completely visited using 5 among the 7 vehicles available.

Vehicle 3 (in cyan), is the only one able to visit sites with high strength of the sea and sites that apply for special equipment.

REFERENCES

Aarts E.H.L., Korst J. (1989). Simulated Annealing and Boltzmann Machines. J. Wiley & Sons.

Bélisle C.J.P. (1992). Convergence theorems for a class of simulated annealing algorithms on Rd. Journal of Applied Probability, 29, pp. 885–892.

Brummit B, Stentz A. (1996). Dynamic mission planning for multiple mobile robots. Proceedings of the IEEE international conference on robotics and automation.

Brummit B, Stentz A. (1998). GRAMMPS: a generalized mission planner for multiple mobile robots. Proceedings of the IEEE international conference on robotics and automation.

Dekkers A., Aarts E., (1991). Global optimization and simulated annealing. Mathematical Programming, 50, pp. 367–393.

Laporte G, Nobert Y, Desrochers M. (1985). Optimal routing under capacity and distance restrictions. Operations Research, 33(5), pp. 1050–73.

Locatelli M., (1996). Convergence properties of simulated annealing for continuous global optimization. Journal of Applied Probability, 33, pp.1127–1140.

Locatelli, M. (2000). Simulated annealing algorithms for continuous global optimization: convergence conditions. Journal of Optimization Theory and Applications, 104, pp. 121–133.

Macharis C, Bontekoning YM. (2004). Opportunities for OR in intermodal freight transport research: a review. European Journal of Operational Research 153, pp. 400–16.

Mitrovi´c-Mini´c S, Krishnamurti R, Laporte G. (2004). Double-horizon based heuristics for the dynamic pickup and delivery problem with time windows. Transportation Research, 28(8), pp. 669–85.

Mole RH, Johnson DG, Wells K. (1983). Combinatorial analysis for route first-cluster second vehicle routing. Omega, 11(5), pp.507–12.

Romeijn H.E, Smith R.L. (1994). Simulated annealing for constrained global optimization. Journal of Global Optimization, 5(2), pp. 101–126.

Ruland KS, Rodin EY. (1997). The pickup and delivery problem. Computers and Mathematics with Applications, 33(12), pp. 1–13.

Ryan, J.L., Bailey, T.G., Moore, J.T., Carlton, W.B., (1998). Reactive Tabu search in unmanned aerial reconnaissance simulations. Proceedings of the 1998 winter simulation conference, vol.1, pp. 873–9.

Toth P, Vigo D. (2002). Branch-and-bound algorithms for the capacitated VRP. In: Paolo Toth, Daniele Vigo, editors. The vehicle routing problem. SIAM Monographs on Discrete Mathematics and Applications, Philadelphia, pp. 29–51.

Wang X, Regan AC. (2002). Local truckload pickup and delivery with hard time window constraints. Transportation Research Part B, 36, pp. 97–112.

Yu Z, Jinhai L, Guochang G, Rubo Z, Haiyan Y, (2002). An implementation of evolutionary computation for path planning of cooperative mobile robots. Proceedings of the fourth world congress on intelligent control and automation, vol. 3, p. 1798–802.

SECURING FREIGHT TRAINS FOR HAZARDOUS MATERIAL TRANSPORTATION: A WSN-BASED MONITORING SYSTEM

Valentina Casola[(a)], Alessandra De Benedictis[(a)], Annarita Drago[(a) (b)], Mariana Esposito[(a) (b)], Francesco Flammini[(b)], Nicola Mazzocca[(a)]

[(a)] Dipartimento di Informatica e Sistemistica
Università di Napoli Federico II
Via Claudio 21, Napoli, Italy

[(b)]Ansaldo STS
Via Argine 425, Napoli, Italy

[(a)]{casolav, alessandra.debenedictis, annarita.drago, mariana.esposito, nicola.mazzocca}@unina.it

[(b)] francesco.flammini@ansaldo-sts.com

ABSTRACT

In recent years the interest in monitoring infrastructures has spread in many application domains, even because of the number of natural disasters and terrorist attacks. This important activity can be seen in the general context of critical infrastructure protection such as the freight train meant for hazardous materials transportation. The design of these systems must answer to several issues: low-cost, easiness of installation, interoperability of information sources, security mechanisms. The use of wireless sensor networks emerged in this field as a compliant solution to these issues. In this paper we will present a monitoring system that uses heterogeneous WSN to monitor a freight train transporting hazardous materials. The sensors interact through a security platform in order to share different information. We illustrate some details on the architecture and the software application to prove the feasibility of such system on a real scenario by discussing most significant results about measurement parameters and networks performance.

Keywords: Wireless Sensor Networks, Security protocols, Data Integrity, Train protection.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are widely used in several critical application domains, as environmental monitoring, detection and classification of objects in military and civil settings, critical infrastructure monitoring and protection, automotive, health monitoring and so on. They can be easily deployed in harsh environments and do not need a supporting infrastructure, thus enabling unattended operations. A typical monitoring system is made of different sensor networks that can be heterogeneous in the technology aspects, in the data formats, in synchronization and localization standards, but also in security mechanisms. They can be connected in different ways and their data should be elaborated by the same application to enrich the knowledge of observed complex phenomena.

Among different critical infrastructures, railway and transportation infrastructures have gone through rapid developments in the last two decades, in several technological aspects including their communication systems. In the past, wired communication systems were used for signalling and data communication in the railway industry, while recently wireless communication systems have emerged as alternatives to substitute wired systems (Lynch and Loh 2006; Li and Wu 2007; Joan, Casas and Cruz 2003; Chebroul, Raman Mishra, Valiveti and Kumar 2008). Wireless systems can be used to monitor and protect critical assets within a railway infrastructure, in order to ensure reliable, safe and secure operations but also to protect citizens from any natural or anthropological hazards (Flammini, Gaglione, Ottello, Pappalardo, Pragliola and Tedesco 2010). New monitoring systems are available in the literature, they are tipically tailored for specific domains and specific technologies, they are not cost-less customizable for new scenarios and they do not easily integrate new technologies or different data models. Furthermore, they usually do not provide any mechanisms to meet security requirements as data integrity and confidentiality that are primary requirements for any critical application domains. We designed a monitoring application based on wireless sensor networks that primary copes with two different aspects: (i) interoperability of different sensor networks (in terms of technologies and security mechanisms), (ii) enforcement of different security mechanisms to provide confidentiality, authentication and integrity of exchanged messages. Within the pShield project (Artemis 2011; Casola, Esposito, Flammini and Mazzocca 2012), we had the opportunity to verify the application and the feasibility of a WSN deployment in a real scenario to protect a freight train. In fact, we installed a WSN on a train available in the Roma Smistamento station and tested our monitoring system. In this paper we will illustrate the architecture of the monitoring system and application by illustrating the main interoperability and security issues we were able to face and, finally, we will illustrate the case study by discussing some experimental results gathered in a real scenario. The remainder of this paper is structured as follows: In Section 2 we will present the motivations and open issues that are behind the choice of adopting Wireless Sensor Network in monitoring transportation infrastructures. In Section 3 we will illustrate a monitoring system that is able to integrate different sensor networks with different security requirements. In Section 4 we will illustrate the results of the experimentation and finally, in Section 5, some conclusions and future work will be drawn.

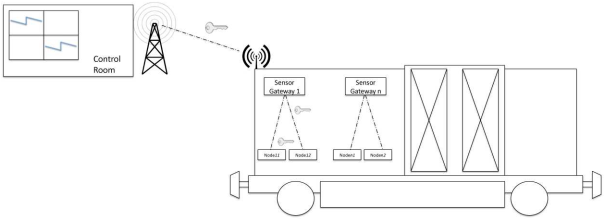


Figure 1: The System View

2. MOTIVATION

In recent years the transport by rail of dangerous goods has increased substantially and consequently the problem of their control and monitoring has became of utmost importance especially if we consider the negative effects and damages that can be caused to people and environment by any accident.

In this regard, the measurement of parameters as acceleration, vibration and position of the wagon could be used to establish if a vehicle is properly moving while temperature and humidity measurement can help to monitor and ensure optimal conditions for the transported goods and/or to prevent the risk of fire. Furthermore, with the adoption of localization tools, as a GPS receiver, it is possible to associate a set of coordinates to an event and send this information for alarm data quality improvement.

Very often, these parameters are measured by sensors already available and deployed, sometimes by new or just installed sensors, both can contribute to the observation of phenomena but there is the need to collect and manage data coming from different and heterogeneous sensor technologies. Indeed, a monitoring infrastructure is a complex system composed of several components, distributed in different points of the infrastructure to protect (e.g. on board train and on the ground) that have to communicate each other to gather the information and properly elaborate them.

In the case of rail domain there are some available solutions, they make use of standard solutions for complex distributed systems and wired sensors available on the wagons, however, in the case of freight trains, there are additional constraints. Indeed, the majority of freight cars are, currently, unpowered hence the need for a power-autonomous system. Furthermore, the railway infrastructures are geographically distributed and some components are mobile, too.

Wireless Sensor Networks (WSN) can be successfully used for such monitoring purposes. In particular, tiny sensors measure different parameters and send results to the gateway, periodically or on demand. The gateway forwards the results to a control center for a further processing and analysis according to a specific application.

In figure 1 the main components that should be deployed to monitor a freight train are illustrated. In particular, we designed different heterogeneous networks deployed inside the car to monitor different parameters with different technologies. They send the retrieved data to a centralized control Room, this collects data and elaborate them according to a specific target application.

The wireless communications for data exchange (both within the sensor networks and between the gateway and control room) should protect data from not authorized access and from other kind of attacks whose aim is to corrupt data integrity.

According to this scenario, we focused our attention on heterogeneity and security issues to design a monitoring system based on wireless sensor networks; unfortunately the solutions for securing data and manage the heterogeneity of data format and syntax available in traditional distributed systems, are not useful in wireless sensor networks because of their resource (CPU, memory, protocols,...) and power constraints.

In the following sections we are going to discuss in details such constraints and open issues, we developed a monitoring system and we deployed it in a real scenario to verify the feasibility of the proposed approach.

2.1. Heterogeneity and security issues

The wide range of parameters to observe (e.g. temperature, humidity, acceleration, GPS coordinates...) could require the deployment of several networks on the car. Such networks could be either legacy and already available or new, each having their proper hardware and software characteristics.

Distributed applications require to collect information from different sources, retrieved data are usually heterogeneous from many points of view (data structure, data format, semantic, protocols, sensing technologies) and they need to be integrated to share the common monitoring objective. Different middleware platforms based on macroprogramming models have been proposed (Hadim and Mohamed 2006; Henricksen and Robinson 2006; Romer 2004; Amato, Casola, Gaglione and Mazzeo 2011) in order to bridge the gap between the application and the underlying hardware and network platforms.

It is plain that security plays a fundamental role in the development of monitoring applications. Data collected by sensors from the environment are sensitive and they should be accessed only by authorized users since a malicious user could attack the network sending corrupted data and compromising the monitoring activity.

Several attacks against WSNs exist and can performed in many ways and at different level (Wood and Stankovic 2002). The communication among sensors is performed via a radio channel which is insecure by nature then this makes a WSN vulnerable to many attacks. Moreover, due to the resource limitation (in terms of energy, memory, computation and communication capabilities) protocols and algorithms proposed for traditional ad hoc networks are not suitable to small sensors (Ravi, Raghunathan and Kocher 2004). Furthermore in most cases, nodes are easily accessible, they can be reprogrammed, replaced or even destroyed. To achieve this goal the WSN must be designed to comply with security requirements such as authentication, integrity and confidentiality; for these reasons new approaches that try to balance security, performance and power consumption are investigated.

The fulfillment of requirements can be achieved primarily by using the cryptography but, due to discussed constraints, not all available schema are applicable: in the Symmetric Key Cryptography (SKC) a unique secret key is used to encrypt and decrypt data, while in Public Key Cryptography (PKC) a pair of keys is used one for each operation.

Until a few years ago the less resource-consuming symmetric schemes were adopted. This choice was dictated by the impossibility to use asymmetric ones (i.e. RSA) (Rivest, Shamir andAdleman 1978) as they are power consuming and require a large amount of computational and storage resources. Recent studies have shown that it is possible to implement PKC to sensor networks by exploiting the primitives offered by the Elliptic Curve Cryptography (ECC) (Kapoor, Sonny and Singh 2008). The strength of this schema is to offer equal security with smaller keys and simpler computations, thereby reducing processing and communication overhead. For example, ECC with 160 bits key provides the same security level compared to RSA with 1024 bits. Some open issues is related to the initial phase of these protocols when the nodes should agree on common secrets to initialize the security mechanisms. We investigated the adoption of different security mechanisms within the WSN, proposed hybrid approaches to cope with open problems and evaluated them from different perspectives (Casola, De Benedictis, Mazzeo and Mazzocca 2011). Among the other heterogeneous features, the monitoring application has to take into account that different networks can enforce different security mechanisms, too.

3. SENSIM-SEC FOR THE PROTECTION OF RAILWAYS

To face interoperability and security issues, we can consider a monitoring infrastructure as composed of two main layers: the sensor network layer and a distributed application layer for the management and elaboration of queries and data. In some previous papers, we introduced SeNsIM-SEC (Casola, Gaglione and Mazzeo 2009; Casola De Benedictis, Mazzeo and Mazzocca 2011), a framework based on a wrapper-mediator paradigm that was designed for integration of heterogeneous sensor networks able to manage the heterogeneity not only in the technology aspects but also in the different security requirements (see Figure 2).

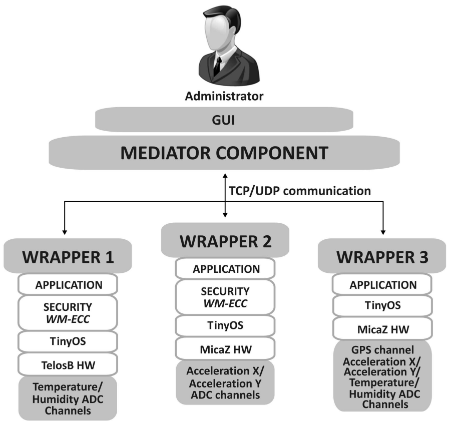


Figure 2: The SeNsIM-SEC architecture for a train

To face interoperability issues, in SeNsIM-SEC, each different network is managed by a dedicated wrapper. It communicates with the specific underlying technology and acts as a connector for the mediator component. The mediator is responsible to properly format user requests and forward them to the different wrappers. Each wrapper translates the incoming queries and forwards them into the underlying networks, retrieves the results and passes them back to the mediator. The communication between the mediator and wrappers is carried out by means of XML files, written according to a standard format and containing information about the structure of the underlying networks, the user-defined query parameters and the retrieved results.

As illustrated in figure 2, the developed architecture for train monitoring is composed of a mediator component, accessible by an end-user via a GUI interface, and of three different wrappers, each managing a different WSN, each of them has specific sensors on board as illustrated in the next section.

When application starts the mediator listens for incoming connections, which will arrive on a UDP Socket bound to a specific port (this information, along with the IP address of the mediator machine is specified in a configuration file which is read by the wrapper component at its startup). When receiving a connection request, the mediator chooses a free port and sends it to the wrapper in a datagram packet . The wrapper uses such port as the remote TCP port to send, via a TCP communication, a struct.xml file containing the specification of the connected network. Each sensor network is composed by two kind of nodes:

1. the master node is responsible of forwarding the queries coming from the wrapper by the UART interface to other nodes, and to send back the result samples;
2. the mote node starts the sensing when they receive a query.

In figure 3 is represented a network example: the node with ID=0 acts as a master and it is directly connected to the Wrapper via a serial interface, it manages the query towards the other nodes of the same network; in this example the mote nodes with ID 4 and 5 are connected via a radio channel to the master and execute the queries by sampling temperature and humidity values.

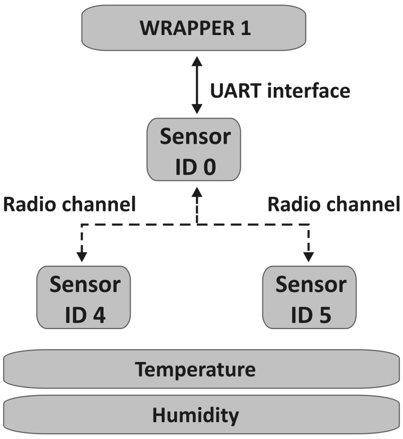


Figure 3: An example of sensor network connection

3.1. Security protocols

To secure the sensor network, security mechanisms were introduced to fulfill nodes authentication, data confidentiality and integrity requirements. These goals were achieved through the use of key exchange agreements, digital signature protocols and data encryption operations, partially provided by the WMECC library (Wang, Sheng, Tan and Qun Li 2007) that implements Elliptic Curve Cryptography (ECC).

WM-ECC is a public available open source implementation of a 160-bit ECC cryptosystem targeted to MICAz, TelosB and Tmote Sky platforms, based on recommended 160-bit SECG (Standards for Efficient Cryptography Group) elliptic curve parameters. The WM-ECC library provides all the ECC operations and some of them are optimized to give the best possible performance; it also provides an implementation of ECDSA (Elliptic Curve Digital Signature Algorithm) protocol but it does not support any key exchange protocol. We aided the application running on nodes with an implementation of the ECDH (Elliptic Curve Diffie Hellman) protocol that allows to establish a unique secret shared key that is used as a symmetric key between the master and the motes for encrypting and decrypting the messages. The encryption and decryption operations are performed by means of the Skipjack cipher, with 80 bit keys and 64 bit blocks.

Figure 4 illustrates the secure communication protocol, putting in evidence the three needed phases:

1. ECDH phase. In the first phase the master and mote nodes exchange their public points to calculate the shared secret key through the primitives provided by ECDH protocol.
2. ECDSA phase. At the arrival of a query, the master node constructs a query message with the received parameters, digitally signs it and then broadcasts it to the mote via radio channel; when receiving a query message, the mote verifies the digital signature and starts the sampling of the required physical values, according to the query parameters, only if the verify procedure is successful, otherwise it discards the message.
3. Encrypt/Decrypt phase. When the results are ready, the mote inserts them into the payload of the response message, which is encrypted with the shared key obtained in the ECDH phase and finally it sends the message to the master; at the arrival of the message, the last extracts the payload, decrypt it with shared key obtained at the first phase and then returns the query results.

We implemented this protocol for securing the communication of all nodes in the networks.

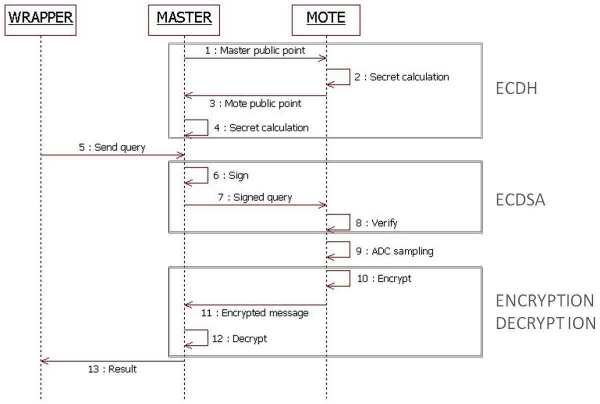


Figure 4: Secure communication protocol

4. THE EXPERIMENTAL CASE STUDY

The SeNsiM-SEC platform was installalled on a freight car made available by the Italian Railway Authority (RFI/Trenitalia) at Roma Smistamento. In figure 5, is showed the car used for the experimentation.

Figure 5: The car outside and inside

The control room was at 30 meters from the stationary train position. As illustrated in Figure 6, on the cars there are 8 sensors, grouped by 2 networks of 3 sensors each and 1 network with 2 sensors (GPS network): one network measures temperature and humidity, one measures acceleration and the third one measures GPS coordinates. On the car there is also the gateway of each network linked to a Wrapper that communicate via a WiFi connection with the control room. In particular, we deployed:

1. A TelosB network inside the car, with humidity and temperature sensors (figure7).
2. A MicaZ network with acceleration sensors, outside the car (figure 8). The outside motes are equipped with a box in order to protect them from bad weather conditions.
3. A MicaZ network with a GPS receiver, installed outside too.

The Wrappers and the Mediator run on different laptops and connected via WiFi, the Mediator and the monitoring application are installed in the Control Room.

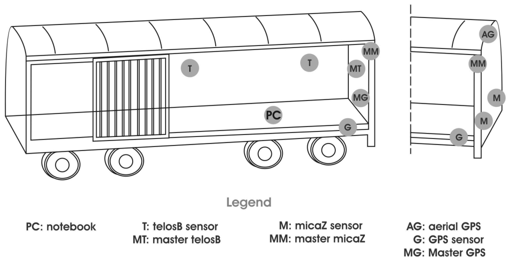


Figure 6: Deployment

We have developed two different applications, respectively for the master and the mote side, they implement a WMECC based security protocol. The master application has been configured in order to digitally sign outgoing query packets addressed to the motes and decrypt the incoming response packets before sending the results to the wrapper. The mote application, in turn, has been configured in order to perform the ECDH protocol initiated by the master, to verify the digital signature of the incoming query packets, and to encrypt all outgoing response packets. The connection among Wrappers and the Mediator implements and SSL protocol.

4.1. Some Experimental Results

In order to test the architecture and demonstrate the functional and security features, different test cases were conduced; we evaluated the parameters sensed by the networks (temperature, humidity, acceleration and GPS coordinates) and we evaluated the packet loss rate on different nodes in two different working conditions:

1. Test 1-Train standing in the station;
2. Test 2-Train running.

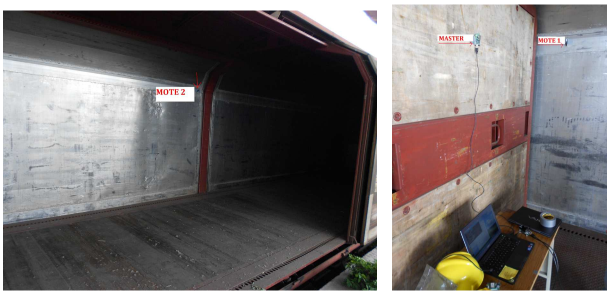


Figure 7: TelosB network

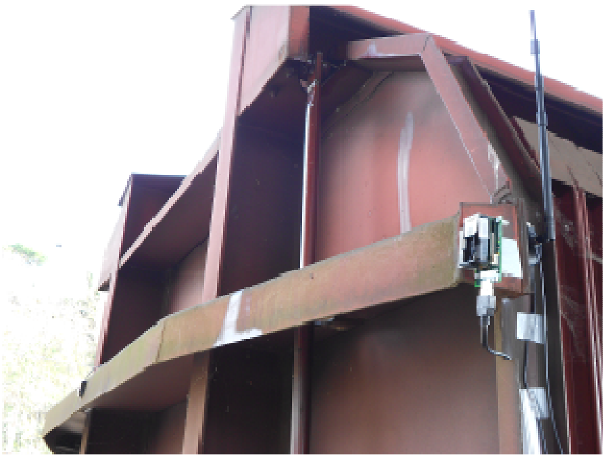


Figure 8: MicaZ network master outside the car

In the following we will illustrate some results of these evaluations, for brevity sake we just illustrate queries concerning only to TelosB network. We want to underline that the goal of this experimental phase was to evaluate the feasibility of the proposed system (WSN hardware and software for the monitoring) and not properly the parameters and values sensed by the different sensors; nevertheless, we will report some of these results, too.

In the Test 1 the train standing in the station. The first test was conducted when the car was standing in the station in order to verify and evaluate the reliability of the connection among nodes; we also evaluated some parameters like temperature and humidity. We assume the TelosB network has two motes with ID 4 and 5. For the first test, we decided to send a query of 5 minutes long (lifetime) with a sample period 0,5 seconds. The network sends back the sensed samples that are collected in a file every 10 seconds (retrieval time) by the wrapper.

Figure 9 shows the evaluated values during the query. The X axis represents the corresponding result file received by the mediator, each result file has samples for 10 seconds of monitoring (retrieval), while the reported values on the Y axis are the mean values evaluated for each file. In table 1 we report the mean values and standard deviation of values for the whole query lifetime and for each sensor. From the result file we can count the number of received samples and easily evaluate the samples loss rate.

Table 1: Sensors mean values

Sensor.Node	Mean	Standard Deviation
Temperature.Node4	19.5 C	0.6
Temperature.Node5	18.06 C	0.8
Humidity.Node4	63.4 %	10.9
Humidity.Node5	61.4 %	4.4

From the result file we can count the number of received samples and easily evaluate the samples loss rate.

According to the query lifetime, the sample period and the retrieval, the mediator should receive 30 result files from network, where the expected number of samples in each of them was 40.

In figure 10 it is possible to see the number of received packets against the expected ones for each node and we evaluated the loss rate of different nodes in the network (figure 11).

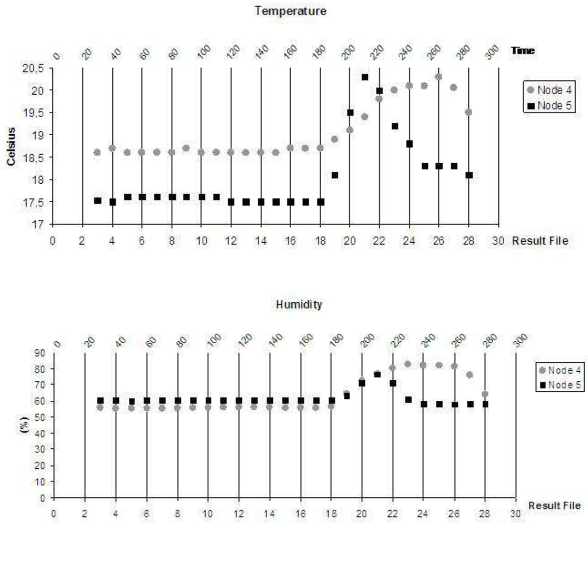


Figure 9: TelosB Network results - Temperature and Humidity

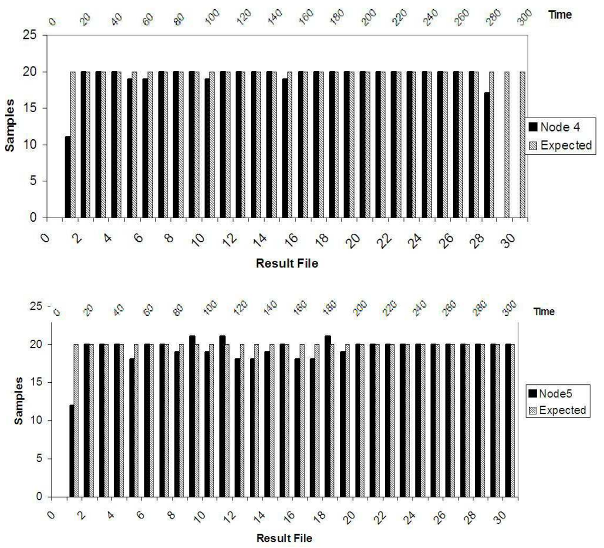


Figure 10: Number of received samples for each node in TelosB

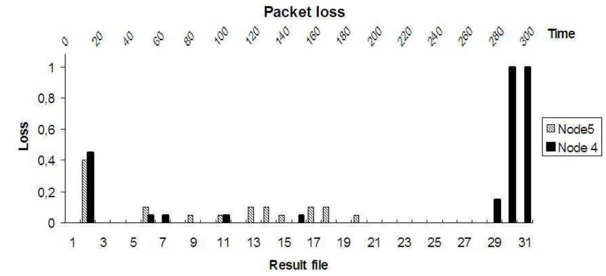


Figure 11: Samples loss rate – TelosB

In table II it is reported the mean number of received samples for each node and for the whole network, evaluated respect of the expected number of samples.

Table 2: Samples Loss

TelosB	Mean
Node4	18
Node4LossRate	9%
Node5	19.4
Node5LossRate	3%
NetLossRate	6%

During the experiment, we decided to stop the node 4, as illustrated in Figure 10 the node loses all samples in the last two files. The node 5 in some intervals has an oversample due to the way SeNSiM aggregates results (e.g. at result file 9, 12 and 18). Both nodes present at the beginning a similar samples loss, this due to the verification of signature in the ECDSA protocol (result file 1).

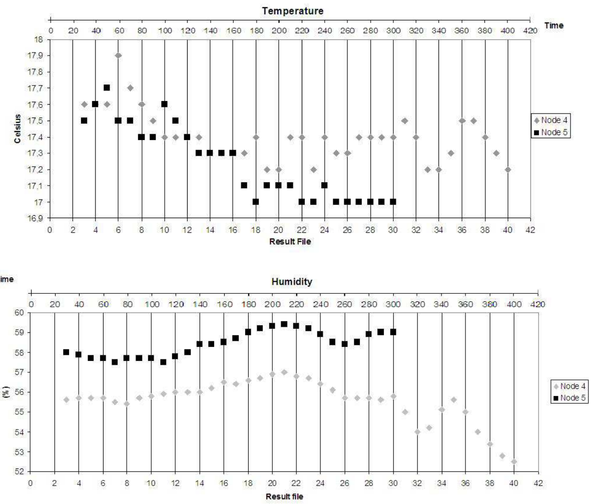


Figure 12: Car in movement – TelosB

In the Test 2 the train is running. The second test was conduced when car was in movement in order to test the connection between nodes and evaluate the measured parameters in a real time condition.

For this test, we sent a query of 7 minutes long (lifetime) with a sample period of 1 second for both networks and 10 seconds of retrieval time. Figure 12 shows the evaluated values during the query for each network.

Again in figure 12 it is reported the case where the Node 5 stacked after the 32th result file and stopped working, this was caused by a not-well closed door that abruptly opened and cut off the node.

In table 3 we reported the mean value and standard deviation of parameters for each network.

Table 3: Sensor mean values for the car in movement

Sensor.Node	Mean	Standard Deviation
Temperature:Node4	17.4 C	0.1
Temperature:Node5	17.2 C	0.1
Humidity:Node4	55.6 %	1.1
Humidity:Node5	58.3 %	0.5

As previously illustrated, we can evaluate the number of received samples and so evaluate the samples loss rate.

According to the query lifetime, the sample period and the retrieval, the mediator should receive 42 result files. For each result file, the expected number of packets for TelosB network was 20.

In figure 13 it is possible to see the number of expected samples for each node and the packet loss rate for the different nodes in the network (figure 14).

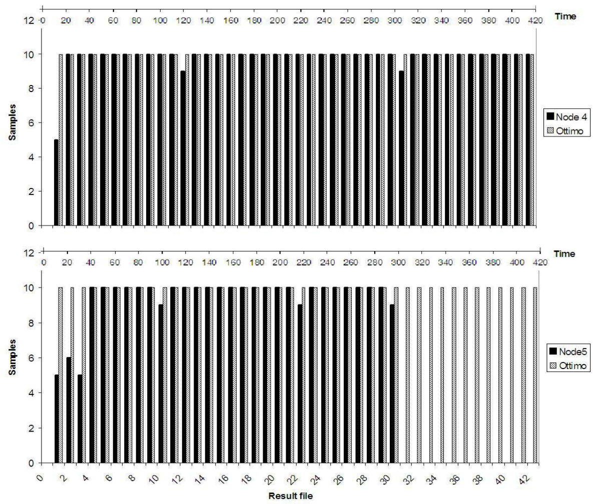


Figure 13: Number of received samples for each node – TelosB

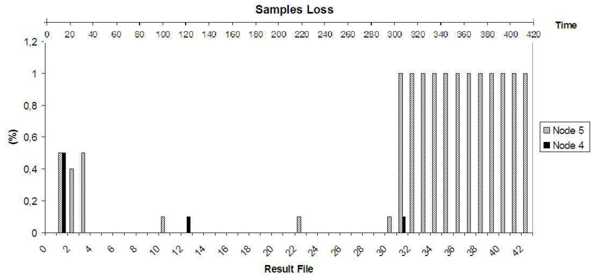


Figure 14: Samples loss rate- TelosB

In table 4 we reported the mean value and standard deviation of parameters for the network under examination.

Table 4: Samples Loss

TelosB	Mean
Node4	9.7
Node4LossRate	2%
Node5	6.6
Node5LossRate	33%
NetLossRate	17%

As the table shows, in this test the network has a good behaviour with a low rate samples loss. Only at the beginning the node lose more samples, always for the ECDSA protocol. We remember that the samples loss of node 5 from 32th result file derives from the accident above mentioned.

5. CONCLUSION AND FUTURE WORK

In this paper we proposed a platform to monitor critical infrastructures as trains. The experimentation performed on the freight car monitoring system provided several useful results. Indeed, we first proved that proposed platform was able to work in a real environment, in presence of harsh operating conditions. Furthermore, the SeNSiM-SEC platform correctly meets the main security requirements by using Cryptography based applications. The security mechanisms do not affect the accuracy of measurements even if a very small delay was introduced in the monitoring activity. Finally, the analisys on network performance was conducted, illustrating that even in running condition, the adoption of wireless sensor networks are feasible on trains. These results motivated our activity and, in next future, we intend to propose more sophisticated monitoring applications based not only on threshold definitions but also on the implementation of decision support systems integrated with available train safety systems.

REFERENCES

A.D. Wood and J.A. Stankovic, 2002. Denial of Service in Sensor Networks, *IEEE Computer,* vol. 35, no. 10, , pp. 54-62.

S. Li, Z. Wu, 2007. Development of Distributed Long-gage Fiber Optic Sensing System for Structural Health Monitoring, *in Structural Health Monitoring*, Vol.6: 133-143.

Kapoor V, Sonny V, Abraham Singh R, 2008. Elliptic Curve Cryptography, *ACM Ubiquity*, 9(20): 20-26.

Joan R. Casas and Paulo J. S. Cruz, 2003. Fiber Optic Sensors for Bridge Monitoring, in Journal of Bridge Engineering, Vol. 8, Issue 6, pp.362-373.

Casola V., Esposito M., Flammini F. Mazzocca N., *2012.* Freight train monitoring: a case-study for the pSHIELD project. *Accepted for publication in the proceedings of the Workshop MCNCS 2012, Palermo, Italy.*

R. Rivest, A. Shamir, L. Adleman, 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *In Communications of the ACM*, 21(2).

Hadim, S., Mohamed, 2006. N. Middleware for wireless sensor networks: A survey. *In: Proc. 1st Int. Conf. Comm. System Software and Middleware (Comsware 2006),* New Delhi, India, January 8-12 (2006)

Romer K. 2004. Programming Paradigms and Middleware for Sensor Networks, *GI/ITG Fachgespraech Sensornetze,* Karlsruhe, Feburary 26-27.

Artemis 2011. *The PSHIELD project*, http://www.pshield.eu/

Casola V., Gaglione A., Mazzeo A., 2009. A Reference Architecture for Sensor Networks *Integration and Management in the Book GeoSensor Networks (Proceedings of GSN)* - Springer, LNCS5659

Srivaths Ravi, Anand Raghunathan, Paul Kocher, and Sunil Hattangady, 2004. Security in embedded systems: Design challenges*, ACM Trans. Embed. Comput. Syst.* , 461-491.

Amato F., Casola V., Gaglione A., Mazzeo A., 2010. A semantic eriched data model for sensor network interoperability, *in Simulation Modelling Practice and Theory* 19(8). Pp. 1745-1757, Elsevier.

V. Casola, A. De Benedictis, A. Mazzeo and N. Mazzocca, 2011. SeNsIM-SEC: security in heterogeneous sensor networks, *SARSSI2011*

K. Chebrolu, B. Raman, N. Mishra, P.K. Valiveti, R. Kumar. BriMon, 2008. A Sensor Network System for Railway Bridge Monitoring, *in Proc. 6th International Conference on Mobile Systems, Applications, and Services (ACM MobiSys08),* Breckenridge, CO.

J.P. Lynch, K.J. Loh, 2006. A Summary Review of Wireless Sensors and Sensor Networks for Structural Health Monitoring, *in The Shock and Vibration Digest,* pp. 38-91.

Henricksen, K., Robinson, R.A, 2006. Survey of Middleware for Sensor Networks: Stateof- the-Art and Future Directions. *In: MidSens 2006: Proceedings of the international workshop on Middleware for sensor networks,* pp. 6065. ACM Press, Melbourne.

F. Flammini , A. Gaglione, F. Ottello, A. Pappalardo, C. Pragliola, A. Tedesco, 2010. Towards Wireless Sensor Networks for Railway Infrastructure Monitoring, *in Proc. ESARS 2010*, Bologna, Italy, pp 1-6.

H.Wang, B. Sheng, C.C. Tan and Qun Li, 2007. WM ECC: an Elliptic Curve Cryptograph Suite on Sensor Motes, *Technical report*, Oct. 30.

A SMART MONITORING SYSTEM BASED ON A FAST CLASSIFIER AND A SEMANTIC POST REASONER

Flora Amato, Valentina Casola, Mariana Esposito, Nicola Mazzocca, Antonino Mazzeo

Dipartimento di Informatica e Sistemistica
Università di Napoli Federico II

{flora.amato,casolav,mariana.esposito,nicola.mazzocca,mazzeo}@unina.it

ABSTRACT

In modern decision support systems there is the need to improve the performance in terms of detection, reliability and real time capabilities. These features are usually in inverse proportion. In this paper we propose an innovative approach for a smart event detection and enriched phenomena comprehension. In particular, the proposed approach is based on a two steps process that tries to quickly identify an alarm and then elaborate the acquired knowledge base with a post reasoner to refine the final decision and give operators more feelings about the situation assessment and raised alarms.

Keywords: monitoring systems, semantic based, knowledge base, sensor data models.

1. INTRODUCTION

The pressing need for territorial protection and for the deployment of suitable disaster prevention strategies has led the protection agencies, as well as the international scientific community, in an effort aimed at the definition of new homeland security strategies and tools. A central activity in any Homeland Security system is the monitoring and observation of different phenomena, aimed at providing an updated and meaningful description of the monitored scenario, as well as its possible evolutions, to enable proper countermeasures for the protection and safety of people and things. In these scenarios, not only smart surveillance and alert systems are needed but enriched decision support systems (DSS) are desirable. Such systems rely on heterogeneous data acquisition tools (sensors, video, historical and simulated data, …) and on data elaboration to prune non significant information; nevertheless, this is not enough as there is the need to interpret what data really represents to reduce false positives and detect even weak alarm conditions. The availability of advanced monitoring techniques and heterogeneous information sources has increased the accuracy in observing, measuring and describing the nature of phenomena: the current level of technology in this field represents an opportunity to improve the understanding about observed phenomena but, at the same time, it introduces a high degree of complexity in the data elaboration and fusion.

Intelligent decision support systems are necessary to enable, when possible, the automatic adoption of countermeasures in case of alarms or to support end users during decision making activities (when a too large number of sensors, devices, or cameras placed inside the site to be protected produce a wide amount of data to be processed). However, many automatic and intelligent detection systems generate unnecessary warnings (false alarms); this problem, unfortunately, severely limits the use of these systems to enable automatic or partially automatic counter-measures. In recent years, scientific world's attention has been devoted to both the information management with information and decision fusion approaches, and to the quantitative reliability estimation of these systems.

On the other hand, to improve the situation assessment, it is possible to adopt different types of models for description of knowledge-base, event correlation and for the definition of the situation and threat identification. Very promising approaches are based on semantic and ontological models.

The semantic model can be used for understanding observed phenomena. In particular all sensors must share the same data model and the same interpretation of data. The data model must provide a syntactic interoperability mechanisms and procedures for semantic enrichment to build models in order to (i) ensure a correct and shared information interpretation, (ii) aggregate raw data into events (simple and composed), that will be used for the situation assessment before a final decision.

In the literature some approaches for event detection and decision support based on semantic inference rules for phenomena comprehension are available. Nevertheless, due to the introduced overhead, the knowledge base is just inferred in offline mode.

In this paper we propose an innovative approach for smart event detection and enriched phenomena comprehension: the knowledge base will be inferred in real time, for the event detection, and a light smart classifier will raise an alarm. The proposed approach is based on two steps:

1. A smart and light on-line inference engine to raise an alarm, in case of threat event detection;
2. A post reasoner off-line inference engine, in order to comprehend the event and its causes.

The former has the task to detect, with real time constraints, dangerous condition, giving a pre-alarm; the latter performs a more complex reasoning activity in order to help users to comprehend the dangerous situation and refine the decision.

The reminder of the paper is structured as follows, in Section 2 some related works are reported, in Sections 3 and 4 a model and relative architecture of the proposed monitoring system are presented. In Section 5 a simple case study on the smart classifier is presented and, finally, in section 6 some conclusions are discussed.

2. RELATED WORKS

In the literature some semantic approaches to manage heterogeneous data from sensors and to infer them for event detection are available. These approaches exploit offline inference in order to extract implicit knowledge from data sensor.

On the other hand, some approaches are beginning to use in line techniques both for enrich the semantic data model and to manage in real time event detection; very often, an offline inference for event comprehension and phenomena analysis is associated.

In (Huang and Javed, 2008) an architecture for sensor information description and processing, named SWASN (Semantic Web Architecture for Sensor Network), is proposed. The architecture is based on four layers: the first is the physical level composed by different sensor networks. Each sensor networks manage its own data format. The data are processed in an Ontology Layer, in which each network has a local Ontology. A Global Ontology is built upon a common vocabulary and it is processed in the Semantic layer for the knowledge extraction, through inference and semantic reasoning. Finally, at user level, it is possible to query the ontology in order to process and elaborate data.

Similar architectures are presented in (Gomez and Laube 2009; Konstantinou, Solidakis, Zoi, Zafeiropoulos, Stathopoulos and Mitrou 2007; Konstantinou, Solidakis, Zoi, Zafeiropoulos, Stathopoulos and Mitrou 2010). In particular in (Gomez, and Laube 2009) and (Solidakis, Zoi, Zafeiropoulos, Stathopoulos and mitrou 2007) an automatic process for transformation of XML data into RDF is proposed, the transformation process is driven by semantic reasoning and mapping rules. The transformation is in real-time but not any detection system is proposed. In (Konstantinou, Solidakis, Zoi, Zafeiropoulos, Stathopoulos and Mitrou 2010) a middleware architecture to manage event detection in real time is presented. It is a middleware architecture for automated, real-time, unsupervised annotation of low-level context features and corresponding mapping to high-level semantics. It enables the composition of simple rules through specific interfaces, which may launch a context aware system that will annotate content without the need for user technical expertise. The middleware has a semantic model only for the event management. There are no models for the data acquired by sensor.

3. A MODEL FOR MONITORING SYSTEM

The proposed approach combine significative results available in literature to enrich data models with semantic information and, at the same time, use a smart classifier to let the detection process be quicker.

A monitoring system can be composed of two main layers: the sensor network and the monitoring system (Casola, De Benedictis, Mazzeo and Mazzocca 2011). As illustrated in figure 1, the sensors network can be, in turn, characterized by: *Sensors Physical Features*, *Measurement Typology* and *Topology*.

The monitoring system, based on inference engines, can be characterized by: *Real Time Acquired Knowledge*, *Real Time Inferred Knowledge* and *Post Reasoner Knowledge*. Each sensor node is responsible to measure specific parameters. The *Sensor physical features* layer models the physical characteristic of a single sensor node and of the whole sensor network.

Measurement Typology layer defines what kinds of measures are gathered from the sensors.

Topology layer models information about the system deployment, describing how the sensors are located in the area of interest.

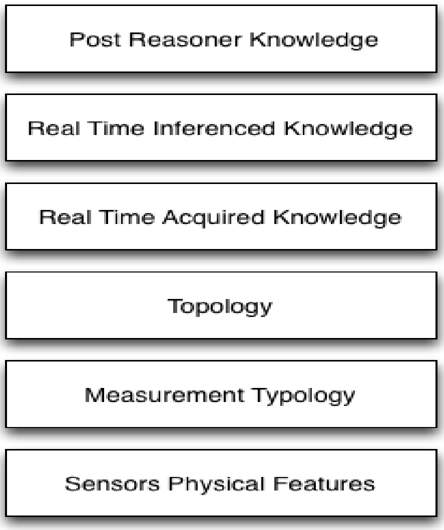

Post Reasoner Knowledge
Real Time Inferenced Knowledge
Real Time Acquired Knowledge
Topology
Measurement Typology
Sensors Physical Features

Figure 1: Model layers for a Monitoring System

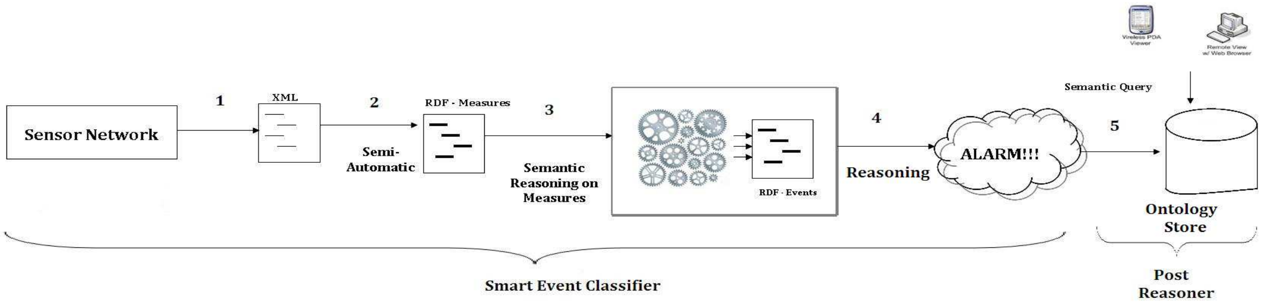


Figure 2: The reference Architecture

The monitoring system acts at two different levels: a real-time reaction and an off-line (post reasoner) activity. The first aiming at providing proper alarms when dangerous events occur, the second aiming at providing a complete and detailed picture of the situation that can be useful for operators both in understanding the situation and for decision supporting.

So, the monitoring system works in these two steps, by means of a fast classifier and through a post reasoner. It can be modelled, in turn, by three layers.

The *Real Time Acquired Knowledge* layer has the task of modeling the typology, the structure and the values of raw and structured data acquired and transmitted by sensors, enriched with semantic information about them (Amato, Casola, Gaglione and Mazzeo 2011). At this level the data is modelled and processed by both the fast classifier and the post reasoner.

The encoding language, used to process and transmit information is the RDF standard.

The *Real Time inferred Knowledge* layer models the knowledge derived by the application, on the sensed data. This level already works on semantically enriched data, the overhead for linking data with information about them, in fact, is necessary at this level because there is a multitude of events that can be detected only by combining information from collections of sensors that are heterogeneous both for typology of measurement carried out and for the data format in which they are sent to centralizer nodes.

Furthermore, at this level, many details on the current situation are abstracted away, in order to allow the classifier to perform efficient decision tasks, even if it is not able to derive the full knowledge about the monitored environment. The cut information is then re-considered into the abstract model of the *Post Reasoner Knowledge*, which works without real time constraints. The *Post Reasoner Knowledge* layer aims at modelling all relevant aspects of the monitored environment. It is focused to derive useful knowledge to have a detailed view of the situation, finalized to :

- help in situation awareness
- support in the decision process.

The acquired data are enriched with RDF semantic information and processed by a reasoner based on Pellet (Kaplanski 2012).

The reasoner is based on a general rules component and a specialist component implementing the rules tuned on the environment to be monitored.

The relevant domain knowledge is encoded with the help of domain experts using appropriate data structures, the ontologies which model the elements of interest in terms of concepts and relationships relating to the phenomena to be monitored, the events and the associated actions to be performed. This ontology is used in order to link each element outputted by the reasoner with a proper descriptions and appropriate information that can be exploited for helping users to understand the situation. The system implementing the semantic reasoner is much more computational expensive than the classifiers used for the real time decisors. At this level, in fact, the outputted inferred data is designed to give support to users with offline reasoning and data mining features, which can be exploited to get a complete knowledge of the situations, even at a later time.

4. REFERENCE ARCHITECTURE

The architecture proposed to implement the proposed monitoring system model, combines different approaches available in the literature. As illustrated in Figure 2, it is composed of:

- A Smart Event Classifier (implementing the Real Time Acquired and Inferred Knowledge layers);
- A Post Reasoner (implementing the Post Reasoner Knowledge layer).

We implemented a fast classifier in order to detect, with real time constraint, potential dangerous condition and then, if necessary, raise an alarm. The events detection is carried out by data correlation coming from different sensors. As a matter of fact, in real situations the potential hazard cannot be detected by using data coming from a single device.

The classifier has a standard structure, composed of learner and predictor components, to build a predictive model and exploit this model for event detection. The predictor is responsible to classify the data collection coming from the sensor network in order to decide if alarm conditions have occurred.

We adopted a rule-based classifier implemented as a decision tree. As usual, in decision tree mechanism, the set of decision rules is modelled as a tree in which leaves represent class associated to the events to be detected and branches represent conjunctions of features, i.e. condition on the sensed data, that lead to those event classes.

In order to define the branch rules domain experts manually classify a sectioned set (training set) of event data. These data are used by the learner module in order to set the predictor parameters, which regulate the automatic detection of the alert conditions. To increment the system performance, the rules have been pruned recurring to a manual refinement made by domain experts (Liu, Ma and Young 2000).

In figure 3 we report a small example of rule codified as a tree branch. The codified rule is:

```
(S1.location = 41°53’24” N, 12° 29’ 32” E,
S1.Pressure > 101.325 kPa,
S2.Pressure > 30 inHg,
S2.location= 41° 53’ 37”N,12°29’11” E)
==>Alarm
```

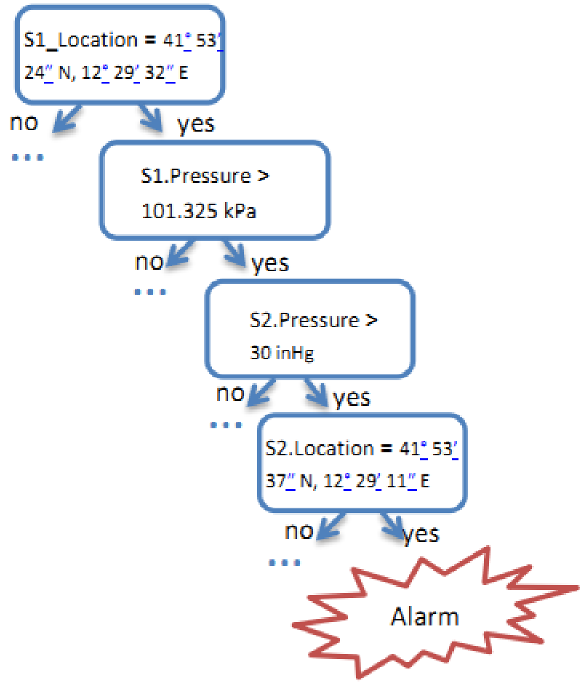

S1_Location = 41° 53' 24" N, 12° 29' 32" E
no
yes
...
S1.Pressure > 101.325 kPa
no
yes
...
S2.Pressure > 30 inHg
no
yes
...
S2.Location = 41° 53' 37" N, 12° 29' 11" E
no
yes
...
Alarm

Figure 3: Tree branch codified Rule

Predictor is realized as a parametric system, whose parameters may vary, or in the presence of new data that affect the system output, or by the intervention of the operator that can decide to manually change them for the occurrence of new conditions.

To fulfil the real time constraints, allowing the system to react in useful time, the classifier may be synthesized in hardware; in particular, in order to manage the variations on the parameters, the predictor is synthesized on a reconfigurable device (FPGA) that allows reconfiguration of the system when is necessary (Wittig and Chow 1996). From a semantic enrichment point of view, the smart Event classifier performs the following actions:

1. Sensor networks gather data and format them in XML files (Konstantinou, Solidakis, Zoi, Zafeiropoulos, Stathopoulos and Mitrou 2010), they encode both sensor properties and measured values;
2. With a semi-automatic activity, XML files are semantically enriched and transformed in RDF files. This file is compliant with the domain ontology and it is suitable to perform semantic reasoning;
3. With the SWRL (Horrocks, Patel-Schneider, Boley, Tabet, Grosof and Dean 2004) language it is possible to perform different inferences to compose simple events in composed ones.
4. On composed events it is possible to detect threats events and generate alarms.

These actions are performed in real time; they also feed the knowledge base for the Post Reasoner component. The just built ontology is stored in a repository (Triple Stores) (Broekstra, Kampman Van Harmelen 2002) and can be used off-line through the adoption of semantic query languages as SPARQL (Prud’hommeaux and Seaborne 2004). Through queries, the post reasoner is able to understand and explain to end users the meaning of the alarms and their causes.

The Knowledge Base can be seen as an information repository about a particular domain of interest. Typical knowledge bases consist of concepts, properties and instances. We encoded the knowledge base using the ontology. The ontology is a set of Classes, Properties and Instances. The Classes define the domain concepts; the Properties define the relation between Classes (Domain to Range). The properties can be between two classes or attributes (a property of a class).

During reasoning, inferences are made, classifying instances of the ontology and associating new properties to instances while maintaining logical consistency.

The reasoner, based on Pellet (Kaplanski 2010), is able to infer logical consequences from a set of asserted facts about the monitoring system defined by user experts. In particular it is composed of two components, one implementing the general inference rules and one the specialist rules, defined by domain experts in order to capture the relevant knowledge about the environment to be monitored.

The system uses first-order predicate logic to perform reasoning. The inferences proceed both by forward chaining and backward chaining (Kaplanski 2010). Not having real time constraints, the post reasoner is not necessary implemented on an embedded system.

5. CASE STUDY

In this section we provide an application of our system for the monitoring of a subway station. The station is supervised through different sensor technologies (Smart-cameras, Infrared Sensors, etc…). The correlation of the different measures, gathered by the sensors, allows to detect some events (e.g. physical intrusions, explosions,…) and, if necessary, raise a proper alarm to the operator.

The station is equipped with a security system including intelligent cameras (*S1*), active infrared barriers (*S2*) and explosive sniffers CBRNe (Chemical Biological Radiological and Nuclear Explosive) (*S3*) for tunnel portal protection. The attack scenario consists of a sequence of simple events which should be detected by the appropriate sensors and combined in order to form the composite event.

The actors of the scenario are defined through instances and they belong to the classes. We implemented an ontology represented in figure 4. This ontology aims at representing the domain of interest, including measures, events and alarms.

Sensor class has a subclass for each device sensor, in this specific case we use an Infrared barrier sensor (IR), a chemical explosive detection sensor (CBRNe) and an intelligent camera (IC) in which are implemented algorithm for video content analysis. The Detect_Event class represents events detected by correlating measurements from the different sensors. Events can be simple or composed. Simple events are related to events detected by single sensors, such as presence of Train detected by smart camera. Composed events are a combination of simple events by means of proper rules. Some composed events can generate an alarm in case of activation. Furthermore, a sensor measures some parameters in order to detect an event; it is characterized by a location and typology. The data properties for some classes are described in table 1.

Table 1: Class and Data Property.

Class	**Data Property: type**
Sensor	ID: int
Measurement	AtTime: DateTimeStamp
Detect_Event	DetectTime: DateTimeStamp

Ontology instances are constantly updated and populated through reasoning operations. The rules allowing the population and enrichment of the ontology are of the following typology:

1. Reasoning on the measures for detect events;
2. Reasoning about simple events in order to generate compounds events;
3. Reasoning on the events for alarms generation.

In this example we show the detection of the "Drop_Explosive_Tunnel" event, regarding the release of explosives in an underground tunnel. In the case of event trigger, a proper alarm must be raised.

Let us suppose that the dynamic of the scenario follows the steps reported below:

1. The attacker stays on the platform for the time needed to prepare the attack, missing one or more trains;
2. The attacker goes down the tracks by crossing the limit of the platform and moves inside the tunnel portal;
3. The attacker drops the bag containing the explosive device inside the tunnel and leaves the station.

A specification for these events is in the following:

- E1. extended presence on the platform (E1 by *S1*);
- E2. train passing (E2 by *S1*);
- E3. platform line crossing (E3 by *S1*);
- E4. tunnel intrusion (E4 by *S2*);
- E5. explosive detection (E5 by *S3*).

The combined event "Drop_Explosive_Tunnel" can be specified in two ways as follow:

1. If (E1, E2) then (E4, E5)
2. If E3 then (E4, E5)

Where E1, E2, E3 and E4 are simple events. The clause "then" states a temporal sequence for the event detection. For brevity, we show the first node activation. The sensed data are firstly codified in XML format (Listing 1 in Appendix), by the centralized nodes implemented in the *Real Time Acquired Knowledge* layer. The listing contains basic information about a sensor, ID, performed measurements, temporal information and value data. In particular, the sensor CBRNE, detecting the presence of an explosive (value = true), is reported. This information is then semantically enriched by exploiting the proper domain ontologies. Starting from the XML, a RDF file is then produced (Listing 2 in Appendix). In the listing the sensor CBRN1, instance of CBRNE class, is reported, it processes information of Chemical type and is positioned in the station 1 (S1). In the same listing CHEM2, instance of the Chemical Class (sub-class of Measurement) is reported. Moreover, the instant of the measurements (AtTime Date) and the value (hasChem) are reported. In this case, the conditions allow the smart classifier to infer the presence of explosive event, in fact, it firstly detects simple events, compose them and raise the alarm condition. The composition of simple events produces the following compounds events:

1. (E1, E2)-> Dangerous_Presence
2. (E4, E5) -> Possible_Explosive

Condition 1 states means, if both events E1 and E2 occur in the same time, then "Dangerous_presence" event is triggered, the second one states if E4 and E5 events occur, the composite event "Possible_Explosive" is detected. The combination, with temporal constraints, of "Dangerous_Presence" and "Possible_Explosive" events triggers the "Drop_Explosive_Tunnel" event, launching the corresponding alarm. In Listing 3 is reported the activation event E5 "Detect_Explosive", triggered by condition on "is_Explosive_Detection". In the second

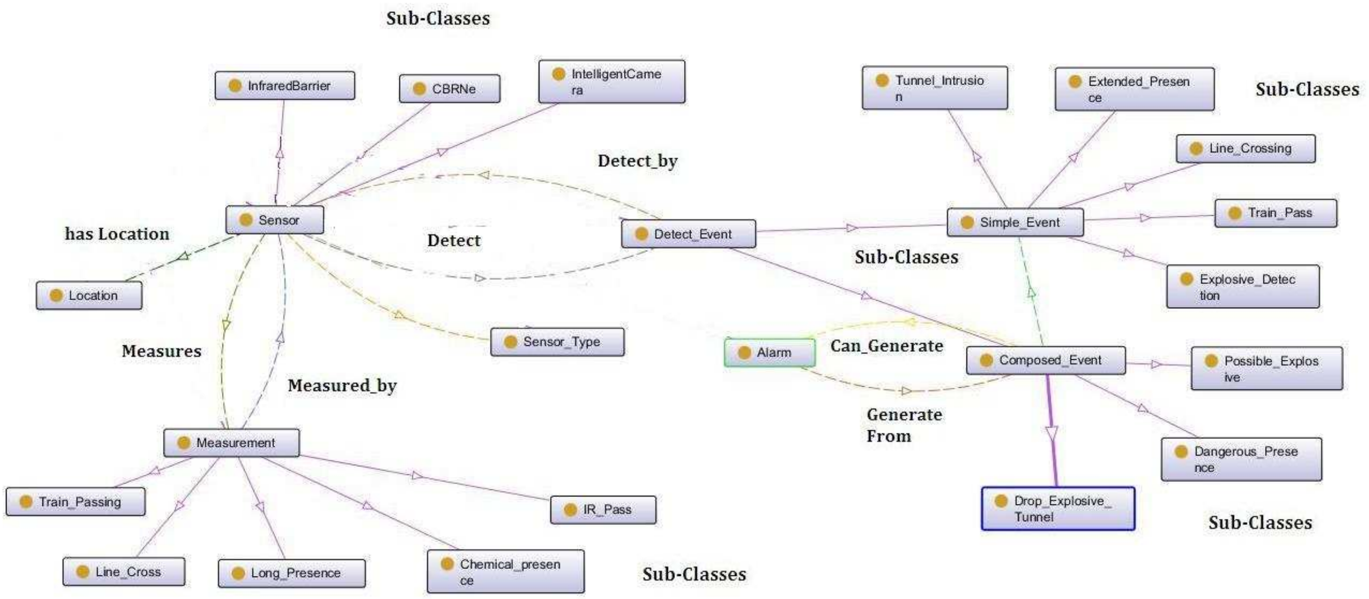


Figure 4: The ontology

part of the listing the event “Drop_Explosive_Tunnel” is composed as composition of “Dangerous_Presence” and “Possible_Explosive” that occur in temporal succession. Finally, Listing 4 shows the activation of the alarm caused by the “Detect_Drop_Explosive” event. The conditions used to manage and understand the cause of the alarms may be queried off-line, through a user friendly interface that exploits SPARQL language for querying the semantic enriched data about the situation, as the alarms that have been triggered and the events detected.

6. CONCLUSIONS AND FUTURE WORK

In this paper we proposed a smart monitoring system based on a two steps process that tries to quickly identify an alarm and then elaborate the acquired knowledge base with a post reasoner to refine the final decision and give operators more feelings about the situation assessment and raised alarms. The proposed approach combine significative results available in literature to enrich data models with semantic information and, at the same time, use a smart classifier to let the detection process be quicker. We have illustrated a simple example, primary focused on the enrichment process to build the knowledge base on which a post reasoner can infer further information for situation assessment. In future works we intend to complete the architecture implementation with this component, too, and use this approach to enrich available decision support systems that are based on different detection models as statistical or mathematical ones.

APPENDIX A - LISTING

```
<?xml version='1.0' encoding='UTF-8'?>
   <result>
    <nodeid value='1'/>
    <location value='Station1'>
    <name value='Chemical_Presence'/>
    <data value='true'/>
<timestampvalue='2012-05-13T09:00:03+01:00'/>
    </result>
```

Listing 1: example of XML sensor output.

```
<!-- http://www.owl-
ontologies.com/Ontology1.owl#CBRN1 -->

 <owl:NamedIndividual
rdf:about="http://www.owl-
ontologies.com/Ontology1.owl#CBRN1">
   <rdf:type
rdf:resource="http://www.owl-
ontologies.com/Ontology1.owl#CBRNe"/>
   <hasType rdf:resource="http://www.owl-
ontologies.com/Ontology1.owl#Chemical"/>
   <hasLocation
rdf:resource="http://www.owl-
ontologies.com/Ontology1.owl#Station1"/>
 </owl:NamedIndividual>

<!--http://www.owl
ontologies.com/Ontology1.owl#Chemical -->

<owl:NamedIndividual
rdf:about="http://www.owl-
ontologies.com/Ontology1.owl#Chemical">
  <rdf:type rdf:resource="http://www.owl-
ontologies.com/Ontology1.owl#Sensor_Type"
/>
</owl:NamedIndividual>

<!-- http://www.owl
ontologies.com/Ontology1.owl#Chem2 -->
 <owl:NamedIndividual
rdf:about="http://www.owl-
ontologies.com/Ontology1.owl#Chem2">
   <rdf:type
rdf:resource="http://www.owl-
ontologies.com/Ontology1.owl#Chemical_pre
sence"/>
   <atTimeDate
rdf:datatype="&xsd;dateTimeStamp">2012-
05-13T09:00:03+01:00</atTimeDate>
   <hasChem
rdf:datatype="&xsd;boolean">true</hasChem
>
 </owl:NamedIndividual>
```

Listing 2: RDF Measure

```
<!--http://www.owl-
ontologies.com/Ontology1.owl#Detect_Explosi
ve -->

 <owl:Thing
rdf:about="&Ontology1;Detect_Explosive">
   <rdf:type
rdf:resource="&Ontology1;Detect_Event"/>
   <rdf:type
rdf:resource="&Ontology1;Explosive_Detectio
n"/>
   <rdf:type
rdf:resource="&Ontology1;Measurement"/>
   <rdf:type
rdf:resource="&Ontology1;Simple_Event"/>
   <rdf:type
rdf:resource="&owl;NamedIndividual"/>
   <Ontology1:is_Explosive_Detection
rdf:datatype="&xsd;boolean">true
</Ontology1:  is_Explosive_Detection>
   <Ontology1:Detect_by
rdf:resource="&Ontology1;CBRN1"/>
   <Ontology1:MeasureFrom
rdf:resource="&Ontology1;Chem2"/>
 </owl:Thing>

    <!--http://www.owl-
ontologies.com/Ontology1.owl#Detect_Possibl
e_Explosive -->

        <owl:Thing
rdf:about="&Ontology1;Detect_Possible_Explo
sive">
            <rdf:type
rdf:resource="&Ontology1;Composed_Event"/>
            <rdf:type
rdf:resource="&Ontology1;Detect_Event"/>
            <rdf:type
rdf:resource="&Ontology1;Possible_Explosive
"/>
            <rdf:type
rdf:resource="&Ontology1;Simple_Event"/>
            <rdf:type
rdf:resource="&owl;NamedIndividual"/>
            <Ontology1:Detect_Time
rdf:datatype="&xsd;dateTime">2012-05-
13T09:00:07+01:00 </Ontology1:Detect_Time>

<Ontology1:is_Possible_Explosive
rdf:datatype="&xsd;boolean">true</Ontology1
:is_Possible_Explosive>
            <Ontology1:Composed_From
rdf:resource="&Ontology1;Detect_Explosive"/
>
            <Ontology1:Composed_From
rdf:resource="&Ontology1;Detect_Intrusion"/
>
        </owl:Thing>
```

Listing 3: Simple and Composed Event

```
<!-- http://www.owl-
ontologies.com/Ontology1.owl#Allarme -->

 <owl:Thing rdf:about="&Ontology1;Allarme">
   <rdf:type
rdf:resource="&Ontology1;Alarm"/>
   <rdf:type
rdf:resource="&owl;NamedIndividual"/>
   <Ontology1:message
rdf:datatype="&xsd;string"></Ontology1:messag
e>
   <Ontology1:message
rdf:datatype="&xsd;string">Attention
Explosive Presence </Ontology1:message>
        <Ontology1335263048:Alarmfrom
rdf:resource="&Ontology1;Detect_Drop_Explosiv
e"/>
```

Listing 4: Alarm

REFERENCES

N. Konstantinou, E. Solidakis, A. Zafeiropoulos, P. Stathopoulos, N. Mitrou, 2010. A Context-aware Middleware for Real-Time Semantic Enrichment of Distributed Multimedia Metadata. *International Journal of Multimedia Tools and Applications* (MTAP), Springer, special issue on Data Semantics for Multimedia Systems, 46(2): 425-461.

Kaplanski, P., 2010. Description logic based generator of data centric applications. *Conference Proceedings of 2nd International Conference on Information Technology* (ICIT),. P 53-56. 2010. IEEE Publishing.

Liu, B., Ma, Y., Wong, C., 2000. Improving an association rule based classifier. *Journal of Principles of Data Mining and Knowledge Discovery.* P.P. 293-317.. Springer Verlag.

Wittig, R.D., Chow, P., 1996. OneChip: An FPGA processor with reconfigurable logic. *Conference Proceedings of IEEE Symposium on FPGAs for Custom Computing Machines P.* 126-135. 1996 IEEE Publishing

N. Konstantinou, E. Solidakis, S. Zoi, A. Zafeiropoulos, P. Stathopoulos, N. Mitrou, 2007. Priamos: A Middleware Architecture for Real Time Semantic Annotation of Context Features. *3rd IET International Conference on Intelligent Environments.*

Gomez, L., and Laube, A. 2009. Ontological Middleware for Dynamic Wireless Sensor Data Processing. In *Proceedings of the 2009 Third International Conference on Sensor Technologies and Applications* IEEE Computer Society, Washington, DC, USA, pp. 145-151.

Amato, F.,Casola, V., Gaglione, A., Mazzeo, A. 2011. A semantic enriched data model for sensor network interoperability. *Journal of Simulation Modelling Practice and Theory.* V 19. N 8. P 1745-1757.. Elsevier

V. Huang and M. Javed, *2008.* Semantic sensor information description and processing. *In 2nd International Conference on Sensor Technologies and Applications.*

Broekstra, J., Kampman, A., van Harmelen, F. 2002. Sesame: A generic architecture for storing and querying RDF and RDF Schema. *In ISWC.*

Horrocks, I., Patel-Schneider, P.F., Boley, H., Tabet, S., Grosof, B., & Dean, M. (May 2004). SWRL: A semantic web rule language combiningOWL and RuleML.

V. Casola, A. De Benedictis, A. Mazzeo and N. Mazzocca, 2011. SeNsIM-SEC: security in heterogeneous sensor networks, *SARSSI2011*

Prud'hommeaux, E., Seaborne, A., 2004. SPARQL Query Language for RDF.

CRITICAL INFRASTRUCTURE PROTECTION: THREATS MINING AND ASSESSMENT

Giusj Digioia[(a)], **Stefano Panzieri**[(b)]

[(a) (b)] Roma Tre University – Via della Vasca Navale 79 – 00146 Rome Italy
[(a)]digioia@dia.uniroma3.it , [(b)] panzieri@dia.uniroma3.it

ABSTRACT

Within Homeland Defense, a crucial aspect is related to Critical Infrastructure (CI) protection. In fact, CIs encompass a wide range of strategic sectors for countries, such as food, water, public health, emergency services, energy, transportation, information technology, telecommunication and finance. Therefore, CIs operation should be granted to ensure national needs satisfaction. In order to monitor and prevent dangerous situations and threats that could affect CIs, Situation Awareness (SAW) theory addresses the goal of maintaining operator awareness, through rough data acquired by heterogeneous sensors monitoring CIs. One of the great problems in SAW is related to the definition of agile models able to highlight threats and to adapt themselves to monitoring requirements. This paper describes how Data Mining (DM) approach can be applied on data acquired by sensors watching at infrastructures, in order to build agile Hidden Markov Models (HMMs), for on-going situation assessment and consequent threat evaluation.

Keywords: critical infrastructure protection, data mining, situation awareness, agile hidden Markov models construction

1. INTRODUCTION

Within the context of homeland security, and in particular in critical infrastructure domain, one of the most felt issue is related to the availability of huge quantities of data acquired by sensors and the incapability to correlate relevant alarms, or to employ them for knowledge model construction that could lead to the definition of preventive actions and countermeasures.

Management of information stored in databases (DB) in order to discover hidden correlations, clusters of data and related descriptions is addressed by Data Mining (DM) discipline; while critical situation recognition and threat evaluation, starting from heterogeneous observations is an issue addressed by Situation Awareness (SAW) doctrine.

Both approaches deal with classification, but DM is generally applied off-line, on a set of data that can eventually be prepared for consequent statistical analysis. Such kind of data structuration leads to the definition of the so-called Data Warehouse (DW), where different classification techniques can be applied. Indeed, SAW manages on-line acquisition of data and try to fit them to a previously defined model, describing the domain of interest. In other words, DM allows extracting distinguishing features of a data; SAW tries to give a meaning to data, explaining why it has been gathered/observed.

The application of both approaches in the same system could be done as follows:

- adopting DM techniques to discover if and how information stored in DBs are correlated to a specific alarm (e.g. "power grid malfunctioning");
- employing mined correlation to build knowledge models, related to most relevant alarms;
- adopting those models for Situation, Threat Assessment and Process Refinement (JDL levels 2, 3 and 4).

Researchers have started to study possible influences between Data Mining and Data Fusion domains only in recently published works.

In McConky [2012] data mining, and in particular an event co-reference process, is adopted to identify descriptions of the same event across sentences, documents, or structured databases. In McConky's work the goal is to understand if different textual descriptions, stored in different DBs, refer to the same event, through the application of a customized event extraction technique and the evaluation of an event similarity measure. Also in the proposed architecture, the correlation between an event of interest and others, stored in different DBs, must be evaluated, but the focus is on causal, temporal and spatial correlation, rather than on similarities. Despite of McConky's work, information managed in our work are properly structured for data mining classification, so that issues related to natural language interpretation are not taken into account. Moreover, while our paper presents an overview of a wide system architecture, in McConky [2012] the focus is on the implementation details of textual event description correlation and user Situation Awareness is supposed to be increased by presenting to him the collection of all existing descriptions of the same event. In this paper, SAW is regarded in a more complex view: user SAW is related to his capability to understand the undergoing situation and to evaluate its threat. With this regard, the proposed system architecture supports the user through the application of inference algorithms on agile knowledge models, which are refined through relations mined in DB records.

In Stark [2012] it is proposed a mixed approach combining data mining and Bayesian Network approach, where BNs are built and validated employing data stored in DBs, and through a refinement process performed by the user. With this regard, Data Mining is meant as a learning process more than a way to discover implicit correlations among data, as instead it is regarded in this work.

In the work of Salerno [2004], from the comparison and analysis of JDL and Endsley's model for Situation Awareness, a new framework for SAW is proposed. Within this framework, Data Mining techniques are mentioned for their potentiality to discover relationships between entities in a database and employ them to generate predictive models capable of describing what has been examined in terms of an abstract mathematical formalism (usually, a graph-theoretic construct). Nevertheless, hints on Data Mining application within the architecture are not deepened.

Another case study in which data mining is applied to SAW is reported in Riveiro [2008], where data mining is integrated with information visualization techniques. The so called *visual data mining* approach aims to integrate the user in the knowledge discovery process using effective and efficient visualization techniques, in order to discover anomalies in maritime traffic.

Finally, Krishnaswamy [2005] presents an Advanced Driving Assistance System that analyses situational driver behavior and proposes real-time countermeasures to minimize fatalities/casualties. The system is based on Ubiquitous Data Mining (UDM) concepts. It fuses and analyses different types of information from crash data and physiological sensors to diagnose driving risks in real time. UDM is meant as the process of analyzing data emanating from distributed and heterogeneous sources, with mobile devices or within sensor networks.

This paper is organized as follows. Section 1 introduces this work, presents its motivations and related works, in Section **Errore. L'origine riferimento non è stata trovata.** an overview of the reference system architecture is described. Section **Errore. L'origine riferimento non è stata trovata.** presents how Data Mining and can be applied to Situation Awareness theory, and in particular for agile Hidden Markov Model definition. Finally Section 4 concludes this paper with remarks and future recommendations.

2. SYSTEM OVERVIEW

In this Section the overview of the reference system architecture is summarized. As mentioned before, the proposed architecture aims to combine Data Mining techniques to inference algorithms, specifically employed for Situation/Threat Assessment and pattern recognition.

The goal of Data Mining is to discover relations among data stored in different and huge databases, and to define clusters of records, characterized by similarities with regard to certain kind of relations. Situation Assessment methodologies allow to recognize situations of interest, observing data acquired real-time from different and heterogeneous sensors.

The link between the two approaches can be summarized as follows: Data Mining approach is employed to define correlations among data stored in databases and events/objects of interest for the user; mined correlations are employed to build knowledge models adopted in the Situation Assessment process.

Data Mining techniques employed in this work refer to *supervised classification*, where main features describing cluster of information are known and algorithm goal is to assess the belonging of data to each cluster. In particular, clusters will be defined according to temporal, spatial and causal relations.

Indeed, Situation Assessment techniques employed in this work refer to *Hidden Markov Model*, able to describe pattern of dynamic/time-dependent situations through a graph of nodes and edges, representing states and relations among them. In particular, the output of the data mining process (i.e. relations among data stored) is employed to build and refine iteratively the Hidden Markov Model adopted in the inference process, where observations from the field feed the model and allow to estimate the on-going situation, to project it and to evaluate its threat, according to the related impact. Finally, relations discovered in the Data Mining phase are regarded as cues for evidence search, contributing to JDL Level 4 functions, i.e. Process Refinement, Hall and Llinas [2001].

2.1. Architecture

In Figure 1 is depicted the overall system architecture. As it can be noticed, the inputs of the system are *observations gathered* from the field and a *Target Of Interest* (TOI), specified by the user. Observations are continuously stored in log databases and feed the Hidden Markov Model employed in the Situation Awareness process; the TOI represents a target of particular interest for a user, such as a specific alarm, a hardware component, or a particular event. When a user is interested in analyzing a specific TOI, to discover everything that could be correlated to it, that need to be under observation, and eventually to prevent related threats/malfunctioning, the user can define a TOI and give it as input to the proposed system.

The outputs of the process are basically a *TOI correlation tree* and a *Hidden Markov Model*. The correlation tree is built by the Data Mining Module that discovers different levels and kinds of correlations among DB records and the specific TOI. The final TOI correlation tree is defined taking into account previous correlation trees built for the same kind of TOI.

HMM is generated by the Agile Model Construction Module, that translates relations discovered among DB records in the states and transitions of the HMM. The HMM is then employed for pattern recognition and threat assessment related to the specific TOI. The system contemplates also an Evidence Search Module, for SAW refinement.

When the system is operative, it manages a set of HMMs and related TOI correlation trees, corresponding to a set of different type of TOIs. Observations are employed to feed HMMs and alert the user about threats related to TOIs. Each time that a specific TOI becomes of greater interest (the user defines it as input of the system), a refinement process is started and leads to HMM and correlation tree refinement. In this way, models of the most critical TOIs are exactly those model most refined, accordingly to stored observations and previous analysis.

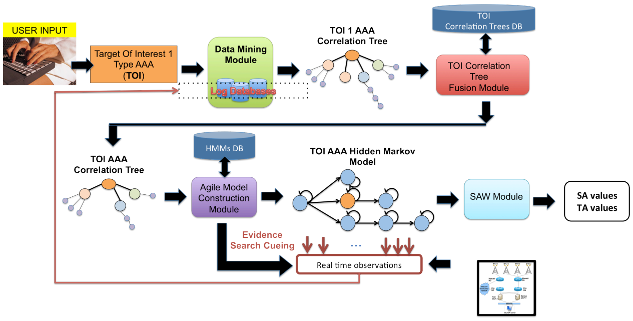


Figure 1 - System architecture

2.1.1. Architecture components

Main components of system architecture are listed below:

Target Of Interest (TOI) – It represents a target of particular interest for the user, as a particular alarm, a particular infrastructure component, a service, a particular event. For interest, we mean the need of the user to gather all correlated information from log DBs, to monitor it, and to prevent possible threats/malfunctioning related to it. The definition of TOIs depends on particular records stored in system DBs. A TOI can be characterized be the following information:

- *Type*: it specifies the typology of a TOI, such as event, component, service, alarm, etc. All TOIs of the same type refer to the same correlation tree and, consequently HMM. For example, "Deny of service" could be the type of the TOI related to a real cyber attack.

- *Name*: it describes the specific TOI.

- *Time*: this field define the temporal information related to the TOI, such ad the date, a time range, etc.

- *Location*: it indicates the geographical location related to the TOI.

Data Mining Module – The main purpose of this module is to mine correlations among records of log DBs and the TOI specified by the user. Data Mining techniques taken into account in this work refers to unsupervised and supervised classification, allowing to define data clusters, accordingly to a set of given variables. The variables chosen in this work express *temporal*, *causal* and *spatial* correlation.

- *Log Databases:* they represent the basis for the data warehouse the Data Mining Module is based on. They could be related to any kind of log, such as alarms, etc., but an intermediate process is required to prepare them to the following kind of analysis:

  - Temporal analysis*:* two records are temporally correlated if the distance between their temporal features is within a specific time range. In particular, different kind of temporal correlations can be defined: given a time interval among day, week, month, year, the records could be fully parallel, partially parallel, consequent.

  - Spatial analysis: two records are spatially correlated if the distance between their spatial feature is within a specific geographic range. In particular, different kind of spatial correlation can be defined: *city, region, country, or areas of different radius*.

  - Causal analysis: two records are causally correlated if the probability that A causes B is higher that a certain threshold δ: $P(B|A) = N_{B,A} / N_A > \delta$, where $N_{B,A}$ is the number of times B occurred within a certain time range, starting from the occurrence of A, and N_A is the total number of times A occurred.

TOI Correlation Tree – A correlation tree represents the tree of all records or TOIs correlated to a specific one, accordingly to at least one of the relations mentioned before. The root of a correlation tree is the TOI specified by the user, the nodes connected to the root with one link represent the 1st level correlated TOIs, the nodes that are distant 2 links from the root, represent the TOIs correlated with the first-level-correlated TOIs, and so on, see Figure 2. The weight of the links expresses the degree of correlation with the up-level node.

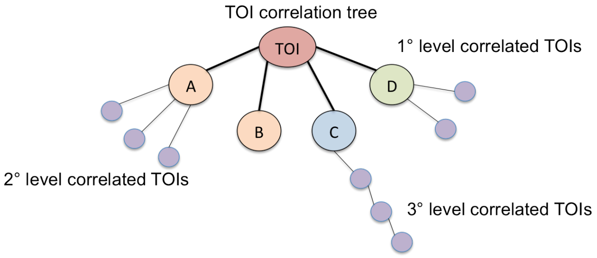


Figure 2 - TOI correlation tree

The size of the tree depends on the size of DBs and on the level of correlation to be investigated. TOI correlation trees can be related to specific TOIs, or to types of TOIs. In particular, the system first generates a specific TOI tree; then the Fusion Module compares it to the correlation tree of the TOI type; finally it updates the correlation tree for the specific type of TOI and stored it as a reference in a proper DB.

Agile Model Construction Module – this module goal is to derive, from the TOI type correlation trees, Hidden Markov Models with which monitor possible threats related to analyzed TOIs. HMMs of interest are therefore those related to TOI type like events or actions (i.e. "power grid malfunctioning"), whose threats need to be evaluated. Translation rules employed to build a HMM from a TOI correlation tree reflect the correlation type and weights mentioned above. In particular tree nodes correspond to the states of the HMM, while transition edges and probability reflects the weight of temporal, spatial and causal correlations among tree nodes. Details of this module are reported in next Section.

Evidence Cueing Module – Once that HMM is defined, a JDL level 4 refinement process can start, that is a process in which sensors and inference algorithms are refined in order to confirm/disconfirm the matching between observed reality and the knowledge model. In the proposed architecture, the refinement process is regarded as cueing the search for evidences that could be hidden to the observation process. In particular, the module highlights to the user the kind of evidence he should look for, accordingly to the type of TOI related to each node of the HMM.

SAW Module – The SAW module task is to take all observations coming from the field and to feed the HMMs stored in the HMM DB, in order to estimate on-going plans related to TOIs. As the approach adopted refers to Markov Theory, the inference process employs the Viterbi algorithm [James 2007], in order to estimate the most probable path, sequence of states, followed up to a certain time, given a sequence of observations. The probability of a certain path corresponds to the Situation Assessment value, expressing the confidence that a certain situation is undergoing. The SAW module then, computes the Threat Assessment value, expressing the impact that a certain situation could have: TA = SA value x damage caused.

In real-time context, two main processes can be identified, the SAW process and the Model Construction Process. The first one runs continuously, feeding HMMs stored in DBs with observations from the field, then archived in log DBs; the latter is triggered by the user, and in particular when he requires the construction and refinement of a specific TOI tree. The Model Construction Process affects the SAW process each time an HMM is updated. As noticed before, most refined models are related to TOIs of greater interest for the user.

3. DATA MINING FOR SITUATION AWARENESS

The process applied by the system at runtime can be summarized as follows:

1. DW update – the variables required for spatial, causal and temporal correlation with the TOI in input are computed, for all the DW records;
2. Unsupervised classification – cluster analysis is applied with regard to the variables added in the DW for spatial, temporal and causal correlation, in order to identify clusters in the DW.
3. Supervised classification – linear discriminant analysis is applied to define discriminant functions of all clusters identified in the unsupervised classification. Discriminant functions in the form of $g_i = \beta_1 x_{1i} + ... + \beta_p x_{pi}$ are computed for each record of the DW, and scores and coefficients are stored for TOI correlation tree construction.
4. TOI tree construction – for each cluster, a threshold is defined expressing the level of correlation of the record with the specific TOI. All records characterized by a score higher than the related threshold is added to at the first level of TOI correlation tree. The edge linking it with the TOI in input is characterized by:

    - The coefficients of the linear discriminant function that express how the record is correlated to the input TOI (for example, if the coefficient of the "Probability that the record is the cause of the specific TOI" is zero, it means that there is no causal correlation between the record and the TOI, while, if it is different from zero, it means that causal correlation exists and depends on the coefficient value).
    - The discriminant function score that expresses how much the record is correlated to the TOI, given the coefficient of the linear discriminant function, i.e. a specific kind of correlation (for example, causal and partially parallel temporal correlation).

The size of the TOI correlation tree can be increased repeating iteratively steps 1-4, using as input TOI a node of the just-generated correlation tree. Tree expansion could require high computation effort for the system, therefore the expansion of the TOI correlation tree should be stopped at the very first levels, sufficient for the proposed system analysis.

A final consideration must be done on TOI correlation tree construction. The frequency with which TOIs are given in input to the system is supposed to be considerably lower than that with which observations are stored in the DW, and cluster analysis is strongly influenced by data employed by supervised and unsupervised classification. This means that new observations could lead to changes in cluster models that are effectively applied only when a specific TOI is given in input to the system. As HMMs for SAW are refined only when a TOI correlation tree is updated, independently by the observation storage process, a HMM will be refined as much as the related TOI is of interest for the user.

3.1. Unsupervised and supervised classification

Data Mining (DM) goal is to select, analyze and model huge quantities of data, in order to discover underlying and hidden relations of specific interest for the DB owner. DM can be regarded as an inductive methodology for information/knowledge retrieval from empirical data to general and theoretic rules to apply in wider contexts, in order to achieve a certain goal, rather than simple knowledge modeling, Nisbet et al. [2009].

In the proposed system, both unsupervised and supervised classifications are applied. Unsupervised classification aims to identify clusters of data accordingly to relevant variables. Usually, in order to identify the most discriminant components, the Principal Component Analysis (PCA) is applied. PCA computes eigenvectors of the correlation matrix and identify those components that classify the best the orthogonal projection of data analyzed. In the proposed system, the variables employed for unsupervised classification are already defined as those computed for causal, temporal and spatial comparison with the TOI specified by the user.

Once clusters of data are identified, through supervised classification, the linear discriminant analysis is applied in order to compute for each record a function of the form: $g_i = \beta_1 x_{1i} + ... + \beta_p x_{pi}$, where g represents the correlation score, and the coefficients are the components of the eigenvector, related to the maximum eigenvalue of the following matrix $D_W^{-1}(D_B)$, where D_W is the matrix expressing the deviation within a cluster, wile D_B is the matrix expressing the deviation between clusters. In order to get a good classification, the expression *Deviation Between/Deviation Within* should be maximized (considering the maximum eigenvalue), exactly how the linear discriminant analysis does. In this way, records of the same clusters are as much as possible similar among them and dissimilar with regard to other records of different clusters.

3.2. Situation Awareness

Situation Assessment is the process whose aim is situations recognition, by employing sequences of observations from the field. Observations usually are gathered from heterogeneous sensors, they are not always synchronized, and they can carry uncertain information. Robust SA techniques can efficiently manage such a kind of observation sequences, in order to fit them into a specific model of the observed reality.

A felt issue in the SA domain is related to model definition and refinement. In fact, if the knowledge model employed does not match with the domain of interest, SA algorithms would never provide relevant results.

In this work, the SA technique adopted refers to *Markov Theory* and contemplates the refinement of the knowledge model on the base of hidden relations existing on data and discovered by the Data Mining Module.

The employment of Hidden Markov Models (HMM) for pattern recognition is motivated by HMM capability to model plans, causal, temporal relations among states and by the existence of well known algorithms for path estimation among model states.

3.3. From Data Mining to HMMs

A crucial aspect of this work is related to the definition of HMMs employed by the system for SA. The task is absolved by the Agile Model Construction Module that is supposed to take in input the TOI correlation tree of a specific type, to look into the DB for the related HMM, and to substitute or to newly generate the corresponding HMM to be employed in SA.

Note that HMMs are generated only for those TOIs representing dangerous events or actions that could be prevented, if adequately monitored. Each time the user considers as relevant a specific event, related HMMs are refined so that they can adapt themselves to new knowledge learnt. The refinement is not strictly limited to parameter tuning, James, Z. [2007], but involves the whole HMM structure, and this is what makes the mentioned HMMs agile.

In the construction of the model, the TOI in input represents the end node of the HMM; to each node in the correlation tree corresponds a state in the HMM; while to each link in the correlation tree corresponds a set of transition edges, accordingly to the cluster correlation model. If a node in the tree is correlated to the TOI in input, this means that it belongs to a specific cluster and that its correlation value is higher than a certain threshold. The model of the cluster is summarized by the coefficients of the linear discriminant function, estimated by the supervised classification. The coefficients are then used to weight and define edges in the HMM.

4. CONCLUSIONS

In this paper a system architecture combining Data Mining with Situation Awareness approaches has been presented. Data mining techniques are adopted to mine hidden relations among data stored in databases. The output of the Data Mining process is then used to build knowledge models employed for situation and threat assessment. Both databases and Situation and Threat Assessment processes are fed with observations gathered from the field.

Data Mining process described in this paper is triggered by the specification of a particular target of interest (TOI) by the user. Once a TOI is given as input, the system Data Warehouse (DW) is updated through the computation of variables expressing spatial, causal and temporal correlation between each record and the TOI itself. Then the unsupervised classification is performed in order to identify clusters of data that are characterized by the same kind of correlation with the specific TOI. When clusters have been identified, the supervised classification, and in particular the linear discriminant analysis, is applied to estimate models of each cluster as linear functions whose coefficients expresses the dependency of the correlation score with the spatial, causal and temporal variables, introduced in the DW.

The output of the Data Mining process (clusters of records and their models) is employed to build Hidden Markov Models for the recognition of situations of interest. The proposed architecture contemplates the refinement of knowledge models each time user requires the analysis of a certain TOI. Therefore, HMMs related to most critical TOIs are also those more frequently refined.

Further works will be addressed to the implementation and validation of the proposed methodology.

REFERENCES

McConky, K., Nagi, R., Sudit, M., Hughes, W., 2012. Improving Event Co-reference By Context Extraction and Dynamic Feature Weighting. *Proc. IEEE Multidisciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, 38-43.

Stark, R.F., Farry, M., Pfautz, J., 2012. Mixed-Initiative Data Mining with Bayesian Networs. *Proc. IEEE Multidisciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, 107-110.

Salerno, J., Hinman, M., Boulware, D., 2004. Building a Framework for Situation Awareness. *Proc. IEEE Information Fusion*, 107-110.

Riveiro, M., Falkman, G., Ziemke, T., 2008. Improving maritime anomaly detection and situation through interactive visualization. *Proc. IEEE Information Fusion*, 46-54.

Krishnaswamy, S., Loke, S.W., Rakotonirainy, A., Horovitz, O., and Gaber, M.M., 2005. Towards Situation Awareness and Ubiquitous Data Mining for Road Safety: Rationale and Architecture for a Compelling Application. Proc. of Conference on Intelligent Vehicles and Road Infrastructure, 16-17.

Hall, D.L. and Llinas, J., 2001. Handbook of multisensor data fusion, *CRC Press*.

James, Z., 2007. *Hidden Markov Model with Multiple Observation Processes*. Honour Thesis.

Nisbet, R., Elder, J., Miner, G., 2009. *Handbook of Statistical Analysis & Data Mining Applications*, Academic Press, Elsevier.

THE USE OF ARTIFICIAL INTELLIGENCE FOR ENHANCED NETWORK DEFENSE

Michael Knight[a], Kortney Raulston[b], Kennard Laviers[c], Kenneth Hopkinson[d]

[a][b][c][d]Air Force Institute of Technology, 2950 Hobson Way, Wright-Patterson AFB, OH 45433-7765

[a]Michael.knight@afit.edu, [b]kortney.raulston@afit.edu, [c]Kennard.laviers@afit.edu, [d] kenneth.hopkinson@afit.edu

ABSTRACT

Even after a network intrusion system (IDS) has identified a cyber-attack, network administrators are still faced with the difficult challenge of assessing network health and status in order to appropriately take action to mitigate damage caused by such an attack due to the large amount of data available from the network components. This paper explores the use of auto-clustering to abstract network meta-data to form high-level units of information that are more comprehensible for a network administrator or an AI Agent to understand and act on. We perform an empirical analysis to evaluate our approach using the NSL-KDD99 dataset for both abstraction of network log data and attack family classification. By auto-clustering, we significantly increase the classification speed without greatly increasing the error.

Keywords: Classification, KDD99, IDS, C4.5, K-Means

DISCLAIMER

The views expressed in this document are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

1. INTRODUCTION

A significant problem with computer networks today is the ability to defend against cyber-attacks in real-time. Defending attacks becomes more difficult when there are an overwhelming amount of network features and samples to analyze. The goal of this research is to detect an attack and formulate a plan to counter the attack as it is happening. The primary focus of this paper will be on the detection portion of the problem. Without the detection of a cyber-attack, the process to create and carry out a plan to mitigate its effects cannot be developed. This plan should include information about the type of attack that is likely occurring in order to produce a set of actions or procedures to combat it. By clustering and classifying network traffic, personnel or monitoring agents can more easily determine if the traffic is originating from an attack or otherwise normal activity. This classifier can be trained on a given network to determine what normal traffic is. Furthermore, if significant features are highlighted before the classifier is created, some of the complexity can be reduced so attacks can be detected more easily. Clustering is the grouping of similar data items into clusters (Fung 2001). In this application, clustering is performed on the individual features of the network trace data so that the important/common features of attack strategies can be highlighted. The data set used is the well-known KDD 99 which is network data produced from a simulated Air Force network experiencing different forms of network attacks. WEKA is a software workbench design to support the application of machine learning technology to real world data sets (Garner 1995). WEKA is useful because of its versatility in allowing data to be presented in its own format, such as the KDD 99 data set, and it is designed to encompass all learning algorithms under a common interface. The algorithms used for this research are ReliefF, clustering by K-Means, and C4.5.

2. RELATED WORK

There has been a great deal of research in the area of learning feature representations from unlabeled data sets for high-level tasks such as classification. Much of this research has shown great progress on benchmark data sets like NORB and CIFAR by making use of complex unsupervised learning algorithms (Coates, Lee, and Ng 2011).

The WEKA system is traditionally used with agricultural data sets and these data sets tend to be larger and of lesser quality than those in machine learning data sets (Garner 1995). Applying the WEKA system to machine learning data sets allows us to answer questions like “Do these changes in certain features indicate a cyber attack?” as well as gain some insight into how to apply learning algorithms to existing real world data sets.

Previously, the classification of network traffic was performed through the use of port-based or payload-based analysis. This has become increasingly more difficult as peer-to-peer networks (P2P) adapt to using dynamic port numbers, masquerading techniques, and encryption to avoid detection (Erman, Arlitt, and Manhanti 2006). To combat these cyber-attack adaptations, an alternative approach for classifying network traffic is introduced by exploiting and extracting common or distinct attack strategy characteristics.

Authors of another related paper (McGregor, Hall, Lorier, and Brunskill 2004) describe their efforts using the Expectation Maximization (EM) algorithm to cluster network flows into different application types with a fixed set of attributes (features). The EM algorithm separates the network traffic into a few basic classes but the accuracy and quality of the clustering is limited due to nature of its fixed attributes. Another technique uses the sequential forward selection (SFS) algorithm (Zander, Nguyen, and Armitage 2005) to find the best feature set to avoid an expensive, exhaustive search. Some other data sets, similar to KDD 99, used with the SFS feature selection algorithm include the Auckland-VI, NZIXII and Leipzig-II traces.

This paper will use the popular and well-known KDD 99 data set for experimentation and evaluation purposes. A modification of the Relief algorithm is used for feature selection and clustering is performed via the K-means algorithm. Additionally, the C4.5 algorithm is used to build a decision tree based on the feature selection results.

3. METHOD

3.1. Data Set

The data set that is used to evaluate the approach introduced in this article is the KDD99 data set. This data set was introduced for the 1999 KDD Cup challenge to accurately classify network data to a given class of attack or normal traffic (KDD Cup 1999). The data set consists of both normal and attack traffic classes, with the attack classes making up the majority of the cases. In total, there are 23 classes and 41 features in the original KDD99 data set (Tavallaee, Bagheri, Lu, and Ghorbani 2009). Later, this data set was transformed into to NSL-KDD99 which solved some issues regarding redundant samples and the over training of classifiers. Dimensions of this data set include measures such as the protocol type, service, server error rates, and byte counts. The values types in the data are nominal, discrete, and real. Attack types include back dos, buffer_overflow u2r, ftp_writer2l, guess_passwd r2l, imap r2l, ipsweep probe, land dos, loadmodule u2r, multihop r2l, neptune dos, nmap probe, perl u2r, phf r2l, pod dos, portsweep probe, rootkit u2r, satan probe, smurf dos, spy r2l, teardrop dos, warezclient r2l, and warezmaster r2l.

Table 1 shows the breakdown of the sample sizes per class in the NSL-KDD99 data set. In this article, only classes with 20 or more samples will be considered due to the difficulty that classifiers have in distinguishing between small sample sizes because they cannot be easily trained to do so. After this modification, there are 14 classes to process and 125,901 samples in all. This is a relatively small decrease as the original sample size was 125,973.

3.2. Feature Selection

Before a classifier is created, only the NSL-KDD99 data set's significant features will be selected. The goal here is to reduce the number of features to be classified so that there are fewer features to process and yet the accuracy is not diminished too greatly. The ReliefF algorithm (Garner 1995) was used to select the best data set features for use by the classifier.

The Relief algorithm, shown in Algorithm 1, is the original algorithm that ReliefF is built upon. The Relief algorithm requires an input n for the number of instances to randomly select and updates the weight values associated with each feature based on choosing the two nearest neighbors. One of these two nearest neighbors is selected inside the class of the randomly selected instance while the other is the nearest outside the class. The ReliefF algorithm slightly modifies the original Relief algorithm by using the nearest k neighbors, where k is specified as an input, in and outside the class. Instead of choosing one nearest neighbor, it chooses k neighbors. This modification reduces the number of random selections of instances needed. ReliefF also allows for any number of classes.

Table 1: Number of Samples, NSL-KDD99 Classes

Item	Type	Count
1	normal	67343
2	neptune	41214
3	werezclient	890
4	ipsweep	3599
5	portsweep	2931
6	teardrop	892
7	nmap	1493
8	satan	3633
9	smurf	2646
10	pod	201
11	back	956
12	guess_passwd	53
13	ftp_write	8
14	multihop	7
15	rootkit	10
16	buffer_overflow	30
17	imap	11
18	warezmaster	20
19	phf	4
20	land	18
21	loadmodule	9
22	spy	2
23	perl	3

The Relief algorithm, shown in Algorithm 1, is the original algorithm that ReliefF is built upon. The Relief algorithm requires an input n for the number of instances to randomly select and updates the weight values associated with each feature based on choosing the two nearest neighbors. One of these two nearest neighbors is selected inside the class of the randomly

selected instance while the other is the nearest outside the class. The ReliefF algorithm slightly modifies the original Relief algorithm by using the nearest k neighbors, where k is specified as an input, in and outside the class. Instead of choosing one nearest neighbor, it chooses k neighbors. This modification reduces the number of random selections of instances needed. ReliefF also allows for any number of classes.

```
set all weights W[A]:=0.0
for i ← 1 to n do
  begin
    select instance of R randomly
    H ← nearest hit
    M ← nearest miss
    for A ← 1 to cardinality(all_attributes) do
      W[A]←W[A]–diff(A,R,H)/n + diff(A,R,M)/n
  end
```

Algorithm 1: Relief Algorithm Pseudocode (Kononenko, Simec, and Edvard 1995)

The primary parameters in WEKA for the ReliefF algorithm are the number of neighbors and the number of instances. The number of neighbors parameter is used to select a given number of neighbors to search in the algorithm. The neighbors include those samples in the randomly selected sample's class as well as the nearest neighbors in the other classes. Because of this, the parameter has to be carefully selected so the number does not go below the smallest total from amongst the classes. The number of instances parameter defines the number of instances to select. In each instance, a random sample is selected and the ReliefF algorithm updates the *weights* of each feature. The *weights* are similar to a scoring feature used to rank the best features and updated according to the equation in Equation 1.

$$W[A]:=W[A]-\frac{diff(A,R,H)}{n}+\sum_{C\neq class(R)}\frac{[P(C)\times diff(A,R,M(C))]}{n} \quad (1)$$

Equation 1 is the ReliefF weight update equation. Please refer to (Kononenko, Simec, and Edvard 1995) for a full description of this derivation.

In feature selection, a greater number of instances will produce the most accurate weights due to the fact that they will approach their steady state values after enough random samples are selected. After the features are selected, a classifier will be built using those features.

3.3. Classification

The data is broken up using a 10-fold validation to test the accuracy of the proposed classification method. The classification was performed with clustering using both the K-Means (MacQueen 1967) and C4.5 algorithms. The K-means algorithm is built upon a very simple foundation: Given a set of initial clusters, assign each point to one of them and each centroid of the cluster is replaced by the mean point on their respective cluster (Fung 2001).

The pseudocode for the K-Means algorithm is shown below (MacQueen 1967):

1. Place K points into the space represented by the objects that are being clustered. These points represent initial group centroids.
2. Assign each object to the group that has the closest centroid.
3. When all objects have been assigned, recalculate the positions of the K centroids.
4. Repeat Steps 2 and 3 until the centroids no longer move. This produces a separation of the objects into groups from which the metric to be minimized can be calculated.

The K-Means classifier is chosen for this application due to its ease of implementation. The number of clusters to be chosen is based on the number of classes in the data set. The goal is to have each class mapped to a cluster using the best features selected by the ReliefF analysis. The trained classifier will then classify a set of test samples and the accuracy will be measured.

Pseudocode for the C4.5 algorithm (Quinlan 1993), also known as J48 in the open source Java implementation in WEKA, is shown below (Kotsiantis 2007):

1. Check for base cases
2. For each attribute *a*, find the normalized information gain from splitting on *a*
3. Let *a_best* be the attribute with the highest normalized information gain
4. Create a decision *node* that splits on *a_best*
5. Recurse on the sub lists obtained by splitting on *a_best*, and add those nodes as children of *node*

4. RESULTS

4.1. Feature Selection Results

Using the WEKA ReliefF implementation, several runs/experiments were performed. We adjusted the neighbor number *k*, and number of instances, *n*. Tables 2-7 shown on the proceeding page depict the top 10 best attributes (features) across multiple values of *k* (number of classes). A feature is considered better if it has a higher correlation to the value being classified.

All instances were used in the data set. There were a total of 125,973 entries. For the number of neighbors *k*, values of two and ten were used. Two is the smallest total quantity for a class. This makes it reasonable to make two the most likely accurate weight. Ten was also used as the number of neighbors with the result having the same top 10 features except with a different order among them. These simulations were rerun with a much smaller set instances chosen at random to see if the same 10 features were selected again.

Compared to the previous three figures, there are no changes in the features displayed after changing *n* from 5000 to 1000 instances. There are, however, some differences in the ordering of the rankings when 1000 random instances are selected, but the same features are all represented in the top ten.

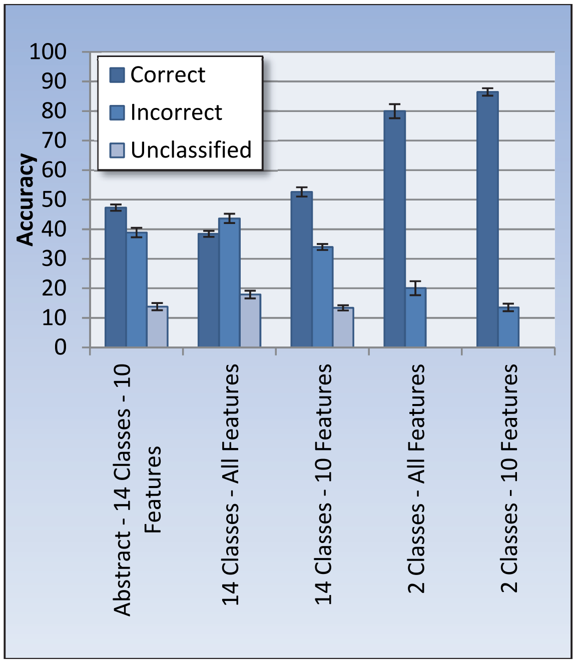


Figure 1: Results from K-Means Varying Classes and Feature Selection

Table 2: Top 10 Best Attribute from ReliefF Using WEKA with k = 10 and n = 5000

Feature Number	Feature Name
3	service
38	dst_host_serror_rate
4	flag
25	serror_rate
26	srv_serror_rate
12	logged_in
39	dst_host_srv_serror_rate
29	same_srv_rate
33	dst_host_srv_count
34	dst_host_same_srv_rate

Table 3: Top 10 Best Attribute from ReliefF Using WEKA with k = 5 and n = 5000

Feature Number	Feature Name
3	service
38	dst_host_serror_rate
4	flag
25	serror_rate
26	srv_serror_rate
29	same_srv_rate
12	logged_in
39	dst_host_srv_serror_rate
33	dst_host_srv_count
34	dst_host_same_srv_rate

Table 4: Top 10 Best Attribute from ReliefF Using WEKA with k = 2 and n = 5000

Feature Number	Feature Name
3	service
4	flag
38	dst_host_serror_rate
29	same_srv_rate
25	serror_rate
26	srv_serror_rate
33	dst_host_srv_count
12	logged_in
34	dst_host_same_srv_rate
39	dst_host_srv_serror_rate

Table 5: Top 10 best attribute from ReliefF using WEKA with k = 10 and n = 1000

Feature Number	Feature Name
3	service
38	dst_host_serror_rate
4	flag
25	serror_rate
26	srv_serror_rate
12	logged_in
39	dst_host_srv_serror_rate
29	same_srv_rate
33	dst_host_srv_count
34	dst_host_same_srv_rate

Table 6: Top 10 Best Attributes from ReliefF Using WEKA with k = 5 and n = 1000

Feature Number	Feature Name
3	service
38	dst_host_serror_rate
4	flag
25	serror_rate
26	srv_serror_rate
29	same_srv_rate
12	logged_in
39	dst_host_srv_serror_rate
33	dst_host_srv_count
34	dst_host_same_srv_rate

Table 7: Top 10 Best Attributes from ReliefF Using WEKA With k = 2 and n = 1000

Feature Number	Feature Name
3	service
4	flag
38	dst_host_serror_rate
29	same_srv_rate
25	serror_rate
26	srv_serror_rate
33	dst_host_srv_count
12	logged_in
34	dst_host_same_srv_rate
39	dst_host_srv_serror_rate

4.2. Classification Results

We use the same number of entries (125,973) for the classification results. The first classifier used for clustering was K-Means. Initially, all features were tested for classification accuracy based on clustering when 14 clusters were chosen. Afterwards, the ten features found by the previous ReliefF calculations were used as a basis for comparison. We found that using the K-Means algorithm (Fig. 1) our classification worked best across all 14 classes using 10 features without the auto-clustering (EM) employed to abstract the feature set. However, switching to the C4.5 algorithm we see the result dramatically boosted by the use of the feature abstraction.

Table 10 shows that the abstraction system classifies the attack type slightly worse on all 14 classes (95% vs. 97%) in the abstracted data-set with a significantly reduced cluster-based data-set. However, as indicated by Table 11 the classifier also acts far quicker (347% faster with K-Means and 48% faster using C4.5) on the simplified cluster-based data set which can be critical in a time-sensitive application.

Table 8: Results from C4.5 Using 14 Classes

	C4.5 –All Features	C4.5 –Ten Best Features
Correct	99.7967%	97.4791%
Incorrect	0.2033%	2.5703%
Unclassified	0%	0%

Table 9: Results Using C4.5and 2 Classes

	C4.5 –All Features	C4.5 –Ten Best Features
Correct	99.7817%	98.487%
Incorrect	0.2183%	1.513%
Unclassified	0%	0%

Table 10: Results Using C4.5 and 14 Classes on Abstract Data Transformed from the EM Algorithm

	C4.5 –Ten Best Features
Correct	95.0811%
Incorrect	4.9189%
Unclassified	0%

Table 11: Time Comparison Using Abstract Features Vs. Normal Feature Set

10 Features, 14 Classes	K-Means	C4.5
Abstracted	5.67	3.69
Normal (in seconds)	25.38	5.49
Improved %	447.62%	148.78%

5. CONCLUSION

This work introduces a new concept of using auto-clustering with the Expectation Maximization algorithm to significantly simplify the feature-set of network traffic along with the use of auto-feature extraction to reduce the number of features. As a result, using the K-Means algorithm our system was able to improve classification speed over 14 classes by over 347% (K-Means) and 48% (C-4.5) clearly indicating this method can be effectively used to improve classification accuracy by a significant margin.

With the methodologies described in this paper, administrators are able to assess a network's health and status more easily. By utilizing the uniqueness of various features in a network, they can be clustered and evaluated to recognize a cyber-attack. There are multiple avenues for future work using auto clustering and feature selection in networks. A more complete version of the KDD99 data set could be used to improve classification results. Success would depend on available computer resources. Experiments using a *k* value of 10% resulted in long algorithm run-times. Another interesting area for future research would be implementing a larger variety classification and feature selection algorithms. For example, the K-means algorithm is relatively simple and easy to implement, but suffers from two drawbacks. First, it is often slow and expensive when used on large datasets and can be sensitive to the initial clusters selections (Fung 2001) which is a stochastic process. Performing a comparative analysis on various classification and feature selection algorithms would provide an indication of which algorithms are more successful in detecting bad network traffic. Furthermore, there are many parameters associated with the algorithms used in this paper and a study to understand how they compare to the current results when undergoing a wider range of experiments would prove useful. Finally, a test benchmark could be constructed to create more realistic data sets than KDD99. This opens up the ability to perform simulated attacks to test the classifier. More accurate classifiers lead to better and more accurate planning and response systems.

REFERENCES

Coates, A., Lee, H., and Ng, N.A., 2011. An Analysis of Single-Layer Networks in Unsupervised Feature Learning, *Proceedings of the 14th International Conference on Artificial Intelligence and Statistics (AISTATS)*, JMLR Workshop and Conference Proceedings, 15.

Erman, J., Arlitt, M., Manhanti, A., 2006. Traffic Classification Using Clustering Algorithms, *Proceedings of the 2006 SIGCOMM Workshop on Mining Network Data*, 281-286.

Fung, G., 2001. A Comprehensive Overview of Basic Clustering Algorithm. *Artificial Intelligence (Computer and Information Science)*, Citeseer press, 1-37.

Garner, S. R., 1995. WEKA: The Waikato environment for knowledge analysis, *Proceedings of the New Zealand Computer Science Research Students Conference*.

KDD Cup, 1999. Data, Available from: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html [accessed 13 July 2012].

Kononenko, I., Simec, E., and Edvard, I.K., 1995. Induction of decision trees using RELIEFF.

Kotsiantis, S.B., 2007. Supervised machine learning: A review of classification techniques, *Informatica,* (31), 249–268.

MacQueen, J.B., 1967. Some methods for classification and analysis of multivariate observations, *Proceedings of the 5th Berkeley Symposium on Mathematical Statistics and Probability*. Available from: http://home.dei.polimi.it/matteucc/Clustering/tutorial_html/kmeans.html#macqueen. [accessed 13 July 2012].

McGregor, A., Hall, M., Lorier, P., Brunskill, J., 2004. Flow Clustering Using Machine Learning Techniques, *Passive & Active Measurement Workshop*, April 19-20, France.

J. R. Quinlan, J.R., 1993. *C4.5: Programs for Machine Learning,* Available: http://books.google.com/books?id=1F1QAAAAMAAJ [accessed 13 July 2012].

Tavallaee, M., Bagheri, E., Lu, W., and Ghorbani, A.A., 2009. A detailed analysis of the KDD CUP 99 data set, *IEEE Symposium on Computational Intelligence for Security and Defense Applications*.

Zander, S., Nguyen, T., and Armitage, G., 2005. Automated Traffic Classification and Application Identification using Machine Learning, *Proceeding of the IEEE Conference on Local Computer Networks 30th Anniversary*, 250-257.

EVIDENCE MARSHALLING WITH INFERENCE NETWORKS: AN APPLICATION TO HOMELAND SECURITY

Ken R. McNaught[a] and Peter Sutovsky[b]

Operational & Decision Analysis Group, Dept of Informatics & Systems Engineering,
Cranfield University, Defence Academy of the UK, Shrivenham

[a]K.R.McNaught@cranfield.ac.uk, [b]P.Sutovsky@cranfield.ac.uk

ABSTRACT

When trying to reason about some adversary's likely intentions, an intelligence analyst frequently needs to combine multiple pieces of evidence observed at different times and having different degrees of relevance, coming from sources with varying degrees of credibility. The evidence marshalling process concerns the structuring of evidence to help analysts and investigators organize their thinking and make better sense of a situation. Here we show how the qualitative structure of a Bayesian network offers a useful approach to evidence marshalling. We propose a framework consisting of four types of nodes, arranged in layers – hypothesis nodes, ground truth nodes, evidence nodes and credibility nodes. An example is presented in the context of homeland security.

Keywords: intelligence analysis, Bayesian network, decision support

1. INTRODUCTION

Not surprisingly, much has been written in recent years about intelligence failures and the need to improve the intelligence analysis process. A good proportion of this is uninformed and unhelpful speculation, grounded in perfect hindsight. However, such a turbulent period affords an opportunity for reflection by the intelligence agencies and it would be surprising if they did not feel that something useful could be learned from recent history.

In addition to the various organizational concerns which have tended to dominate the discussion, another potential avenue for improvement which has been suggested relates to the analyst reasoning process. While Heuer (1999) raised awareness of the potential deleterious effects of various cognitive biases on intelligence analyst reasoning some years ago, recent events, along with a generally wider acceptance of how important such cognitive effects can be (as witnessed by Daniel Kahneman's Nobel Prize for Economics in 2002, for example) have shone the spotlight back in this direction.

Following from Kahneman's observations of two modes of human reasoning, Wastell (2010) provides an excellent discussion of how these relate to the intelligence analyst. The natural reasoning mode can be viewed as a mixture of instinct and experience. When making decisions in this mode, we are making use of our gut feel for a situation and any experience we might have acquired of similar situations in the past, what Klein et al (1986) refer to as recognition primed decision-making. However, it can be shown that over-reliance on this natural reasoning mode quickly leads us astray. For example, many relatively simple problems involving probability or everyday calculations often defy our intuition. Furthermore, it is well known that most people's ability to process more than a few pieces of information at a time is severely limited (Miller 1956). When required to combine several pieces of information, this leads us to take shortcuts. In some repetitive, regular situations this may be sensible and lead to acceptable results but in others, particularly new situations where we may have little experience and where there is much uncertainty, it will lead to sizeable errors and misjudgements. It is in these situations where we need to employ our second 'systematic' mode of reasoning based on logic and rationality.

Furthermore, Wastell (2010) argues that it is here where there is a lack of formal methods to complement an analyst's in-built natural reasoning capability. Without such methods and sufficient training to accompany them so that they become second nature when required, analysts can end up over-relying on natural reasoning.

Evidence marshalling is the name usually given to methods which attempt to organize evidence in some systematic fashion, typically to aid sense-making and to support decision-making by analysts or investigators relating to the case in question. In this paper we outline an approach to evidence marshalling based on inferential networks. This builds on the work of Schum (2001) who has been instrumental in developing a science of evidence. In the next section, we consider this and related work. The following sections discuss a generic framework and present a particular example in the context of homeland security.

2. EVIDENCE MARSHALLING

An item of evidence has several characteristics. These include relevance to the issues being addressed, source credibility, particularly where human intelligence is involved, and timeliness or latency, since typically we might expect a newer observation to carry greater weight than an older one of the same type. In conflict situations when trying to reason about some adversary's likely intentions, it is frequently necessary to combine multiple pieces of evidence observed at different times and having different degrees of relevance, coming from sources with varying degrees of credibility. Identifying unreliable sources can be particularly important in reducing vulnerability to deception, as is identifying common or highly dependent sources. In such high-stakes situations, the pressure on investigators can be very high.

While traditionally, these investigators were largely expected to rely on their experience and intuition to make sense of a situation, there is now increasing interest in providing them with some form of decision support. This in no way diminishes the value of experience or the need for intuition. It simply recognises the scale of the task faced by the investigator and attempts to supplement their capabilities by utilising modern technology.

One relatively well-known method of systematic analysis, proposed by Heuer (1999) to overcome confirmation bias in particular, is Analysis of Competing Hypotheses (ACH). In uncertain situations, there are usually several plausible explanations for an action or an observation. From these, we can select a number of alternative competing hypotheses. However, human nature tends to make us look for evidence which confirms our favourite hypothesis rather than that which would disconfirm it or support other hypotheses. We might also place more weight on evidence which confirms our favourite hypothesis and less weight on evidence which casts doubt on it. The result is that we often stick with our early favourite hypothesis for too long, even when considerable disconfirming evidence is building up.

In relating items of evidence to multiple competing hypotheses, the intention is to keep minds open, and avoid getting stuck in a favoured hypothesis too early. Of note is the emphasis of the approach on the importance of negative evidence (i.e. the definite absence of some indicator) and the varying diagnosticity of different pieces of evidence, i.e. how well a given piece of evidence can discriminate between the hypotheses under consideration.

While it could certainly be claimed that ACH is a form of evidence marshalling, this latter term usually signifies a more comprehensive approach to relating evidence and hypotheses. For example, in the experimental, visual analytic 'Jigsaw' system (Stasko et al. 2008) developed to help intelligence analysts navigate a vast array of potentially relevant documents, provision is made for a 'shoebox' which is essentially an evidence marshalling tool. Such a tool can help an analyst to organize the available evidence, so aiding the construction of a coherent case.

The evidence marshalling process, described by Schum (2001), concerns the structuring of evidence to help investigators organize their thinking and make better sense of a case. It can include creative elements related to the construction of narratives or explanations, the identification and analysis of evidence gaps, and notions of evidence thresholds to take different actions. In the case of homeland security, these could include more intrusive surveillance or making an arrest. The potential for deception must also be considered explicitly (Elsaesser and Stech 2007).

Schum (2001) outlines a number of methods in tiers of varying complexity concerned with organizing evidence. One of the more complex is the Wigmore chart (Wigmore 1937). This was devised by the legal scholar John Wigmore in order to map the structure of a legal argument. As Schum rightly observes, such a construct bears considerable similarity to a particular type of modern probabilistic graphical model, usually known as a Bayesian network (Pearl 1988 and Jensen 2001). Although there are significant differences, both can be described as inferential reasoning networks.

In this paper, we explore the potential for Bayesian networks to be used as a tool for evidence marshalling in the context of homeland security. As well as organizing existing evidence, such a tool can help to encourage thinking about new avenues of enquiry, and highlight gaps in the evidential support for a hypothesis. With often very limited resources, support is required to identify the most promising lines of enquiry. In our view, decision aids such as the inferential reasoning networks presented here can help in such situations. Furthermore, they can help to address some of the problems and limitations encountered in the communication of uncertain information in the intelligence field as described, for example, by Weiss (2008).

3. PROPOSED FRAMEWORK

Figure 1 displays a proposed, generic inferential reasoning network. This consists of four layers of nodes: high-level hypotheses, expected ground truth activities related to these hypotheses, evidence (or perhaps its absence) relating to the expected activities, and finally evidence credibility nodes which help in distinguishing evidence collected from different sources.

The kind of propositions contained in the first three layers bear some similarity to the three levels of propositions discussed in forensic science – namely, crime level, activity level and source level (Taroni et al, 2006). In that domain, hypotheses at the crime level tend to revolve around the guilt or innocence of one or more suspects.

In the intelligence domain, the first layer of nodes contains the key, high-level hypotheses of interest to the analyst, e.g. the target of a planned attack, the intentions of a suspected terrorist cell or the role of an individual in a terrorist organization. In each of these situations, there will be several possibilities, corresponding to the multiple competing hypotheses in the ACH method. While alternatives which are truly mutually exclusive would normally be accommodated within a Bayesian network as different states within a single hypothesis node, for this kind of application we propose that each competing hypothesis is explicitly represented as a separate node in the network. This makes the analyst keep the full set of possibilities in mind at all times and makes it easier to follow which items of evidence and sources relate to which hypotheses.

The second layer of nodes contains variables which represent a number of activities typically associated with the hypotheses under consideration. These should reflect the modus operandum of the terrorist organization and provide a bridge between the hypotheses and the observable evidence. Nodes in the second layer are usually considered to be not directly observable themselves, i.e. there might always be an element of doubt about their truth or falsity.

Here we have referred to nodes in the second layer in Figure 1 as ‘ground truth’ nodes. This is intended to convey the notion that such variables effectively describe the true nature of the situation. However, that, of course, is typically hidden from us for a long period of time and some ground truth variables may always remain a matter of dispute and never be revealed. As in the forensic science domain, we expect nodes at this level to most often be associated with activities of various types, e.g. training recruits, making explosives, and preparing for an attack.

In contrast, evidence nodes in the third layer correspond to observations that have been made or can be realistically expected to be made in a useful timeframe. Their observation, or for that matter lack of observation, will depend in a probabilistic sense on one or more ground truth variables. Nodes in this layer are directly observable and cover the gamut of evidence types including human intelligence, signals intelligence, imagery, etc. It is when we become aware of such evidence that we revise our beliefs in the second layer nodes and then, in turn, revise our beliefs in the top-level hypotheses. Naturally, some items of evidence will lead to greater revisions than others. Furthermore, an item of negative evidence, i.e. the definite lack of some expected indicator, should also lead to appropriate revisions in our beliefs.

The final set of nodes we have labelled ‘credibility’ nodes. Each evidence node which has been observed is associated with a corresponding credibility node. These recognise that some pieces of evidence are more trustworthy than others. This might be because of the source of the evidence, e.g. an experienced field agent vs an unknown informant vs an informant with a long track record. It can also reflect the circumstances in which the evidence was collected. A credibility node has not been attached to all evidence nodes. This is because some of them are simply included as potential evidence nodes which have not yet been resolved. The lack of some evidence item might be due to that item not having been searched for or because after searching it has not been found. Only in this latter case have we associated a credibility node with the absence of the item, which is then an observation in its own right. In these cases, the credibility rating would reflect both the difficulty and the thoroughness of the search. It is much more likely that an observed absence of an evidence item reflects its genuine absence when an exhaustive search has taken place rather than a superficial one.

In terms of its structure, this type of network is qualitatively the same as a Bayesian network (Pearl, 1988). As such it is possible to quantify the nodes with probability distributions to facilitate true probabilistic inference. However, this would require the elicitation of many uncertain probabilities and so is not recommended for routine application, although there may be occasions when it is desirable. Nonetheless, the BN’s qualitative structure provides a logical framework for qualitative reasoning.

Within our proposed framework, both evidence nodes and credibility nodes can be opened within the software tool we are developing to store and retrieve information deemed relevant to them. For example, an evidence node may contain a detailed description of the evidence itself, the identity or other information about the source of the evidence, and links to relevant documents or images. A credibility node may contain information about the source’s track record and the chain of custody which the item of evidence has experienced. Based on these, some overall assessment of the evidence’s credibility may be recorded. Essentially this should moderate the extent to which our beliefs in higher level ground truth and hypotheses nodes are updated in the light of this item of evidence.

The workspace shown below the network represents the type of information that an analyst is prompted for by our prototype tool. This is a free text area which allows the investigator to record their beliefs as time progresses and evidence unfolds. There are three main categories – a summary of the analyst’s current understanding of the situation, an analysis of evidence gaps and key uncertainties, and finally a list of actions required. This is intended to encourage thoughtful reflection as the evidential picture unfolds, as well as the explicit recognition and analysis of evidence gaps, contradictions and uncertainties, including possible deception activities by the adversary in question. Finally, the investigator is invited to make a list of required actions such as requests for additional information, requests for resources, suggested new leads to investigate, current leads to drop, etc, based on the foregoing analysis. This helps to create an audit trail, which can be time-stamped, of what was done, when and why during the course of an investigation, clearly linking these decisions with the beliefs and possibilities being considered at the time and providing a logical justification for them. Such an approach also supports collaborative working, making it easier for co-workers and shift workers to understand each other and pick up where the other one has left off.

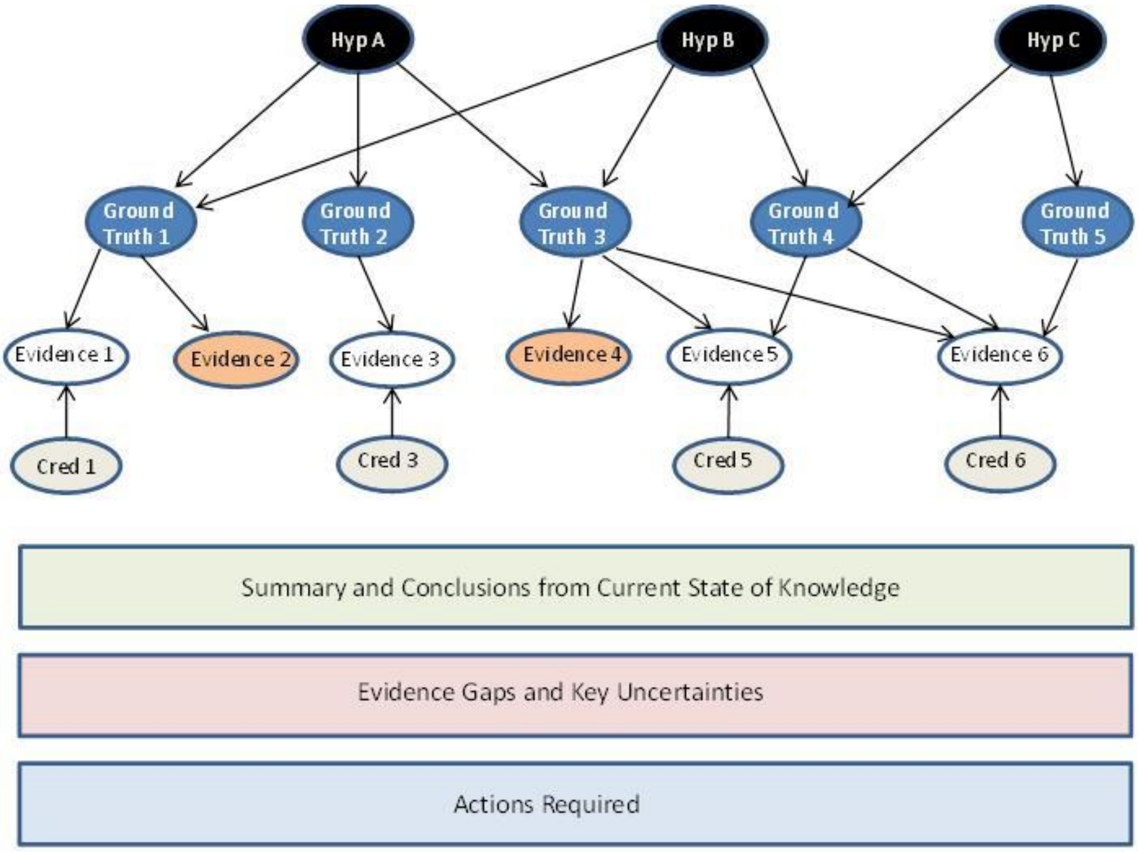


Figure 1: Generic inferential reasoning network and associated workspace.

4. EXAMPLE APPLICATION

In this example, an intelligence agency is concerned with a potential threat from a known terrorist organization. They have become concerned with a high level of chatter, the nature of which is often symptomatic of an impending attack by this organization. Furthermore, they have recent human intelligence that an attack is to be mounted by this organization on a particular target (here denoted as Target A). The source of this intelligence (here denoted as Source 1) is considered credible by the agency and has provided correct intelligence about this organization in the past. A separate source (Source 2) has also provided intelligence of an impending attack by the same organization but has not identified a specific target. In response to the received intelligence, the agency has examined CCTV footage relating to target A. This has identified some suspicious activity some time ago consistent with possible reconnaissance on Target A. However, there is no evidence of a recent dry run on this target. Rudner (2009) describes elements of the modus operandum for Al Qaeda attacks on infrastructure targets. This kind of information is useful in identifying activities to include in the second layer of nodes.

The specific items of evidence which need to be considered by the intelligence analyst in this example are as follows:

- High level of Chatter observed, consistent with impending attack somewhere
- HUMINT received from Source 1 that an imminent attack is planned on Target A
- Source 1 has previously provided HUMINT that person X belongs to organization Z
- Search through CCTV in vicinity of Tgt A reveals possible reconnaissance some time ago.
- No recent evidence of further reconnaissance or dry run observed.

This evidence set would lead to an inferential reasoning network along the lines of that presented in Figure 2. An imminent threat to Target A is the most obvious hypothesis to consider. However, an alternative explanation might be that Target A is part of a deception, a decoy for an attack on a different target. Yet another hypothesis is that no imminent attack is planned and the supporting evidence for an attack is mistaken, possibly due to errors and misunderstandings or possibly the result of a deliberate hoax. Multiple explanations or hypotheses such as these should be considered for the evidence available so far, and expanded or contracted as necessary. As new hypotheses are considered, these generate ideas for possible new items of evidence and new avenues of enquiry.

The workspace below the network in this example might point to the lack of evidence suggesting pre-attack planning on any target other than A. This may lead to an action to request a search of relevant CCTV footage in the vicinity of other likely alternative targets. The human intelligence from Source 1 is key and needs to be scrutinized. In addition, the accuracy of previous intelligence provided by this source needs to be checked. In this example that relates to the information that individual X belonging to organization Z. Obviously, the more correct information that X has previously provided, the higher is the credibility of any new intelligence that they provide. Also relevant, however, is the ease of attainability and usefulness of the previously correct intelligence. A source who regularly contributes correct and useful intelligence which is difficult to obtain should expect a higher credibility rating than one who provides intelligence which is less useful and more widely available.

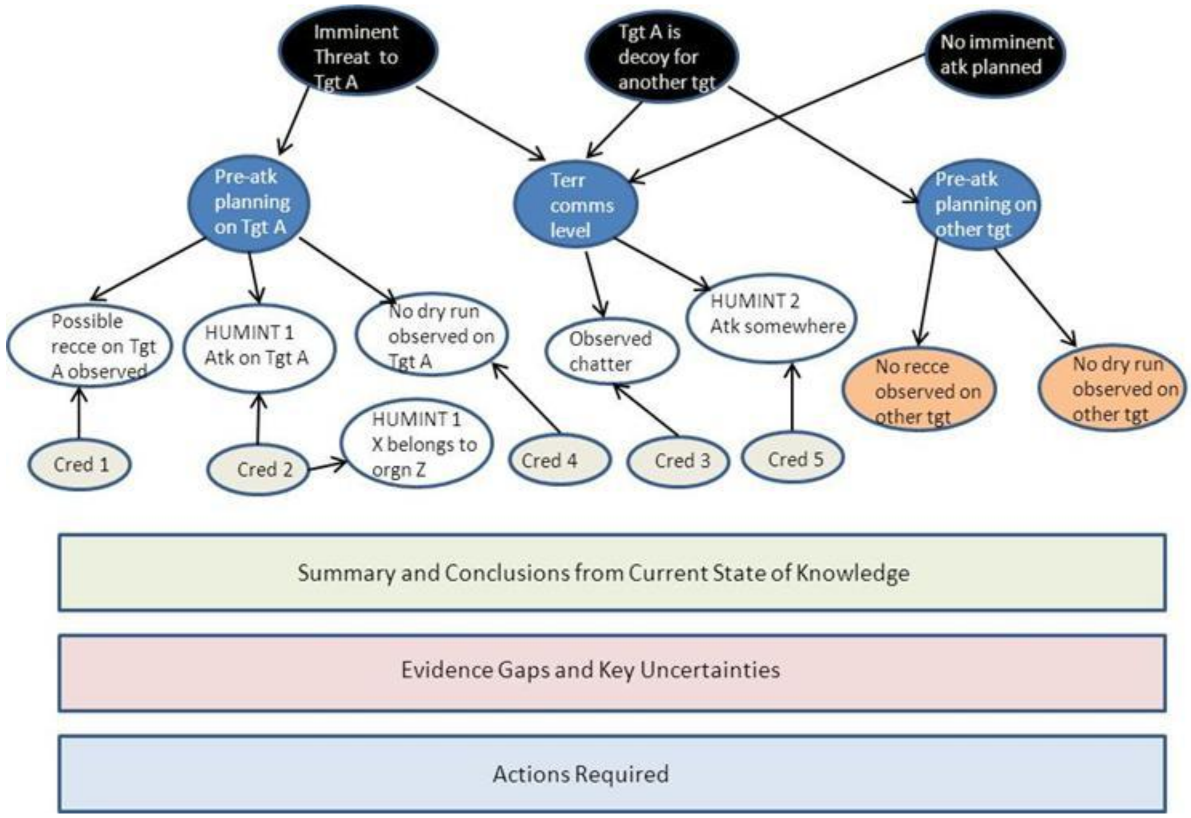

Imminent Threat to Tgt A
Tgt A is decoy for another tgt
No imminent atk planned
Pre-atk planning on Tgt A
Terr comms level
Pre-atk planning on other tgt
Possible recce on Tgt A observed
HUMINT 1 Atk on Tgt A
No dry run observed on Tgt A
Observed chatter
HUMINT 2 Atk somewhere
No recce observed on other tgt
No dry run observed on other tgt
Cred 1
Cred 2
HUMINT 1 X belongs to orgn Z
Cred 4
Cred 3
Cred 5
Summary and Conclusions from Current State of Knowledge
Evidence Gaps and Key Uncertainties
Actions Required

Figure 2: Specific example inferential reasoning network and associated workspace.

5. CONCLUSION

Experience and intuition will always be invaluable core ingredients for reasoning and decision-making in the domain of intelligence analysis. However, that does not obviate the requirement for more formal tools to support an analyst's systematic mode of reasoning. Inexperienced analysts, in particular, may benefit from such support. In this paper, we have highlighted the potential of Bayesian networks to provide a logical and intuitive approach to support an analyst's reasoning process. In particular, we have suggested a framework consisting of four types of nodes, emphasizing the distinction between observable evidence nodes and typically unobservable ground truth nodes. However, in the approach outlined here we have made no use of the quantitative aspect of BNs - that will be explored in a separate paper. Our purpose in this paper is to demonstrate that even without explicit probability distributions, the qualitative support to logical reasoning provided by BNs can still be substantial. Such inferential reasoning networks show how hypotheses, propositions and observations or evidence are related and offer a useful framework for collaborative working and reasoning under uncertainty. Such a framework also supports explicit consideration of an adversary's deception activities, an aspect which will also be developed further in a future paper.

ACKNOWLEDGMENT

The authors are grateful for funding provided by the UK's EPSRC under Grant Number EP/H023135/1.

REFERENCES

Elsaesser, C. and Stech, F., 2007. Detecting deception. In: Kott, A. and McEneaney, W.M., eds. *Adversarial Reasoning – Computational Approaches to Reading the Opponent's Mind*. Boca Raton, FL: Chapman & Hall, 101-124.

Heuer, R., 1999. *The Psychology of Intelligence Analysis*. Washington DC: Center for the Study of Intelligence, CIA.

Klein, G.A., Calderwood, R. and Clinton-Cirocco, A. 1986. Rapid decision making on the fire ground. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 30(6), 576-580.

Miller, G.A., 1956. The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review*, 63, 81-97.

Pearl, J., 1988. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. San Mateo, CA: Morgan Kaufmann.

Rudner, M.,2009. Protecting critical energy infrastructure through intelligence. *International Journal of Intelligence and Counter-Intelligence*, 21, 635-660.

Schum, D.A., 2001. Evidence marshaling for imaginative fact investigation. *Artificial Intelligence and Law*, 9, 165-188.

Stasko, J., Gorg, C. and Liu, Z., 2008. Jigsaw: supporting investigative analysis through interactive visualization*.* *Information Visualization*, 7, 118-132.

Taroni, F., Aitken, C., Garbolino, P. and Biedermann, A., 2006. *Bayesian Networks and Probabilistic Inference in Forensic Science*. Chichester: Wiley.

Wastell, C.A., 2010. Cognitive predispositions and intelligence analyst reasoning. *International Journal of Intelligence and Counter-Intelligence*, 23, 449-460.

Weiss, C., 2008. Communicating uncertainty in intelligence and other professions. *International Journal of Intelligence and Counter-Intelligence*, 21, 57-85.

Wigmore, J.H., 1937. *The Science of Judicial Proof: As Given by Logic, Psychology and General Experience and Illustrated in Judicial Trials*, 3rd ed. Boston, MA: Little, Brown.

AUTHORS' BIOGRAPHIES

Ken R. McNaught is a senior lecturer in Operational Research (O.R.) at Cranfield University's School of Defence and Security situated at the UK's Defence Academy in Shrivenham. He leads the Operational and Decision Analysis Group where his research interests include simulation, combat modelling and decision support, particularly making use of probabilistic graphical approaches such as Bayesian networks and influence diagrams. He also teaches on a number of specialized MSc courses, including Military Operational Research and Defence Simulation and Modelling.

Peter Sutovsky is a research fellow in the Operational and Decision Analysis Group at Cranfield University's School of Defence and Security in Shrivenham. He is currently finishing a PhD in the area of probabilistic graphical modelling for disease outbreak detection in the University of Pittsburgh's Department of Biomedical Informatics.

APPLICATION OF UML FOR RISK BASED INTERDEPENDENCIES MODELLING IN CRITICAL INFRASTRUCTURES

Anatolijs Zabasta [(a)], Oksana Nikiforova [(b)], Nadezhda Kunicina [(c)]

[(a)] M.oec.ing., Riga Technical University
[(b)] Dr.sc.ing., Riga Technical University
[(c)] Dr.sc.ing., Riga Technical University

[(a)] Anatolijs.zabasta@rtu.lv, [(b)]Oksana.nikiforova@rtu.lvl, [(c)] Nadezda.kunicina@rtu.lv

ABSTRACT

This paper presents a systematic approach for computing metrics and performance indices of interdependent critical infrastructures based on their information content, expert views and risk analysis capabilities. The paper also proposes a risk-based methodology based on generic risks and assurance levels using security properties: availability, confidentiality and integrity. Unified Modelling Language (UML) is proposed in order to define a model for research of critical infrastructures interdependences.

Keywords: Critical infrastructures, modelling, Unified Modelling Language.

1. INTRODUCTION

The safety, security and reliability of critical infrastructures are strongly governed by interaction phenomena. Direct dependency mechanisms are relatively easy to identify, model and analyze in very small portions of critical infrastructures. However, in the case of multiple, large-scale critical infrastructures, direct dependencies between elements form loops and give rise to mutual dependencies, i.e., interdependencies (Setolaa, Porcellinise, and Sforna 2009).

Most researchers represent a generic view at critical infrastructure (hereafter abbreviation CI will be used) and its services interdependencies, which supports overall concept, but not rather practical for real world. Therefore an approach that aware heterogeneous nature of CI interrelating at observed territory (for example city, region) is needed.

Let us assume that each critical infrastructure is composed of services that are provided to customers. Services may be self-contained or may depend on other services, which may be provided by the same or by another service provider. Current risk analysis methods do not provide a way to share risk knowledge between providers forming CI. Usually providers have expertise on risks on their own infrastructure, but not on related infrastructures of other providers. Also, since different critical infrastructures are very divergent in nature, risk data gathered from particular infrastructure cannot be easily interpreted by non-domain experts.

In this work is presented an approach that allows monitoring critical infrastructures by considering the state of the services as well as the states of interdependent services. This can be achieved by abstracting data gathered from the CI to a common set of parameters that can be shared with interdependent infrastructures.

We also propose an application of the Unified Modelling Language (UML) in order to define a model for research of CI dependences. The approach taken in applying of the UML has been towards establishing a fair basis for multi-agent modelling and simulation of critical infrastructures. However simulation of critical infrastructures is not a task of this work.

The approach described in this work could help service providers allocated in neighbourhood to make more qualified decisions and to plan risk mitigation actions. Furthermore the ontology proposed in this work can be readily adapted to other cases, taking into account the specifics of each city.

The paper is structured as follows. Authors summarize the related work in the area of CI analysis and describe the difference of their own ideas from the results presented in previous researches. The essence of the approach offered in the paper is expressed in Section 3, which details main steps proposed by authors for monitoring of the state of CI and their interdependent services. An example of dependence of water supply and telecommunication services from the outages happened in power grid is described in Section 4. The main contribution of the research, general results and possible directions for future work are discussed in the conclusion of the paper.

2. RELATED WORKS

Casalichio and Galli (2008) presents a taxonomy that classifies interdependency metrics on the basis of their information content, decision support and risk analysis capabilities, and computational costs. A risk-based methodology that aims to monitor interdependent services based on generic risks and assurance levels which allows determining the security state of a critical infrastructure service is described in Aubert, Schaberreiter, Incoul and Khadraoui (2010) work.

A MICIE project among other objectives had a task to develop methodologies, algorithms and tools to perform quantitative evaluations of risks and threats deriving from interdependencies existing among CIs (Project MICIE 2010). In Rinaldi (2005) work critical infrastructures and their interdependencies are analyzed and different suitable modelling techniques are discussed. Dependencies can be either to one of the other services identified during the decomposition or to a service provided by another CI (Schaberreiter at al. 2010).

CI security modelling approach was presented in (Aubert at al. 2010; Aubert, Schaberreiter, Incoul, and Khadraoui 2010). The aim of the approach is to transform real-world infrastructure information into common abstract risk related information.

A risk-based methodology that aims to monitor interdependent services based on generic risks and assurance levels using security properties: confidentiality, integrity and availability were demonstrated in Zabasta and Kunicina (2012) work.

Bagheri and Ghorban (2006) proposed an extension to the Unified Modelling Language (UML) in order to define a model for research of CI dependences and a fair basis for multi-agent modelling and simulation of critical infrastructures. UML multi-agent model that captures the static structure and dynamic behaviour of a water distribution networks was presented by Lin, Sedigh, and Miller (2010).

3. METHODOLOGY

The goal of the presented approach is to address the challenge of monitoring of the state of critical infrastructures and their interdependent services. Our hypothesis is, that it is possible to reduce the complexity of a service through abstraction to a common (risk related) set of parameters. This enables to compare critical infrastructures designed to serve very different purposes (energy, telecommunication, water supply, transport and etc.) and composed of very different infrastructure components. It enables also to monitor important system parameters like availability, confidentiality and integrity. The abstraction to a small set of common parameters will encourage service providers to share them with interdependent providers.

The authors used considerably adjusted methodology described by (Aubert, Schaberreiter, Incoul and Khadraoui 2010; Schaberreiter at al. 2010; Zabasta, Kunicina 2012).

The four modelling steps are detailed as follows (see Fig. 1):

- Service components assurance and risk assessment;
- Measurement aggregation;
- Services interdependencies linking
- CI interdependencies modelling using UML

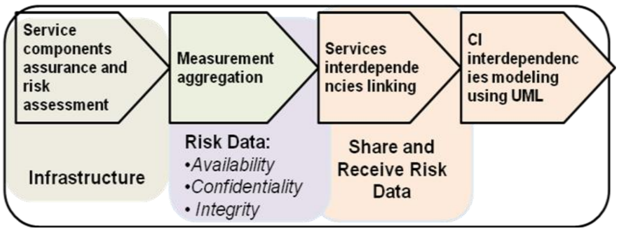

Service components assurance and risk assessment
Measurement aggregation
Services interdependencies linking
CI interdependencies modeling using UML
Infrastructure
Risk Data:
•Availability
•Confidentiality
• Integrity
Share and Receive Risk Data

Figure 1: Four Modelling Steps of CI Interdependences

3.1. Service Components Assurance and Risk Assessment

The first step of the offered methodology relies on a risk analysis of the concerned infrastructure to determine services that can be considered as critical. During this first step, the following activities should be conducted: critical services identification, interdependencies identification, base measures identification, metrics composition and interdependency weighting.

Critical services identification activity aims to identify services within the scope of the infrastructure that may be considered as critical. A critical service is a service for which failure to comply with confidentiality, integrity or availability would eventually undermine global functioning (e.g. QoS) of the infrastructure. Once the services are identified, all the assets contributing to the service’s goals should be identified. This identification consists of a detailed inventory of components used directly or indirectly by the service.

For interdependencies identification the list of identified critical services and components is utilized. This activity aims to identify all the relationships (dependencies or interdependencies) between services. The scope of this identification covers internal dependencies (within the infrastructure) as well as external dependencies (between services of other infrastructures). Domain experts with advanced knowledge of the infrastructure can implement this activity. In addition, external dependency identification may require extracting information documents like contracts or close collaboration with other infrastructures owners.

Base measures identification activity aims to define relevant measures for each identified critical service extracted from the system components. Such base measures can be for example sensors outputs, intrusion detection systems outputs, etc. Taking into account heterogeneous nature of infrastructure components an assurance level is associated with each measure. In order to define a particular level, a specific scale is applied: ISO 15408-1:2009 (2009), ISO/IEC 27001:2005 (2005). This scale is composed of five assurance levels excluding quite not reachable levels as the two last levels (EAL6 and EAL7).

Metrics composition: In order to produce unified values for each service measure, measures associated to a same service are assembled in metric form. Such metrics can be assembled in criterion form, thus each service can be characterized by only three criteria:

- Confidentiality: absence of unauthorized disclosure of information concerning the data transmitted by the critical service;
- Integrity: absence of improper system state alterations concerning the critical service;
- Availability: readiness for correct critical service.

Each measure will be used at least to produce one indicator. In this purpose composition weights in terms of confidentiality, integrity and availability (C, I, A) are associated to each measure (W_{μ_i}). This weighting allows taking into account various measures diversity in terms of influence. These weights will be used during metric risks level and assurance level determination of the metric. Assurance level of the metric is determined using the following formula (the result is rounded to the nearest integer):

$$AL_m = [\sum_{i=1}^{n} (AL_{\mu_i} * W_{\mu_i})] / [\sum_{i=1}^{n} (W_{\mu_i})], \qquad (1)$$

where m is a metric, μ is a measure, AL_{μ_i} is the assurance level of the measure μ_i, n is the number of measures composing and $W_{\mu i}$ is the weight of the measure μ_i.

Interdependency weighting is based on interdependencies identification, thus domain experts describe each dependency in terms of confidentiality, integrity and availability by assigning respective weights. These weights should represent the local impacts of service degradation on related services.

3.2. Measurement Aggregation

This step aims to perform periodic measurement on critical services, in order to estimate the overall risk levels for the three security criteria

Normalization: The normalization process transforms heterogeneous data into normalized data that can be compared and processed using a five levels scale. The determination requires a thorough knowledge of the considered service area and therefore is realized by an expert or a group of experts. Decimal discrete data is normalized as follows: a reference value is defined for each measure. This value is used to compute the measure deviation towards the expected value, expressed as a percentage. In parallel, threshold values are defined in order to classify values into the following classes: not reached: 1, weak: 2, acceptable: 3, correct: 4 and reached: 5.

Metrics risk level aggregation: At the next step normalized measures will be composed into metrics by aggregation. The aggregation formula is based on weighted-sum and enables to obtain a reasonable estimate of the metric risk level. The expected value is an integer between the smallest “1” and the highest “5” risk level as defined above. The following formula is used to determine a single risk level value for a metric, which will be rounded to the nearest integer value:

$$RL(m_x) = (RL_M + 1) - [\sum_{i=1}^{n} (NV(\mu_i) * W_{\mu_i})] / [\sum_{i=1}^{n} (W_{\mu_i})]$$

, (2)

where m_x is a metric, RL_M is the maximum risk level, n is the number of measures for the metric, $NV(\mu)$ is the normalized value of μ, μ is a measure and $W_{\mu i}$ is the weight of the measure $\mu_\text{i.}$

Criterion aggregation: After having determined the risk level of each metric, the various metrics can be aggregated into criterion. Metrics composing into criterion have a specific weight (W_mi) given by domain experts, that specified the importance of each metric in the criterion building. Thus, the adopted aggregation method is a weighted mean using these weights. Criterion risk level will be computed using the following formula:

$$RL(C) = [\sum_{i=1}^{n} (RL(m_i) * W_{m_i})] / [\sum_{i=1}^{n} (W_{m_i})], \qquad (3)$$

where C is a criterion, m is a metric, $RL(_{mi})$ is the risk level for the metric m_i, W_{mi} is the weight of the metric m_i and n is the number of metrics for the criterion.

In order to obtain an integer value, this two previous computation results are rounded to the nearest integer value.

3.3. Services Interdependencies Linking

Using the weighted interdependency functional model, each CI service will send normalized criteria risk levels coupled with respective computed assurance levels. A service that receives a pair of criteria risk and assurance levels can use them to compute a risk linked to its dependencies. For example we can consider critical infrastructure with services S1, S2 and S3, which require a service S_P from electrical power supplier. Since services of involved CI have been described and evaluated in the same measure system, the dependency weight values should be assigned to each dependency $S_P \rightarrow$S1with W_1, $S_P \rightarrow$ S2 with W_2 and $S_P \rightarrow$S3with W_3. In case of interdependencies of several infrastructures and services this analysis will be considerably more complex.

3.4. Interdependencies modelling using UML

The increasing role of modelling in software system development promotes a methodology, mostly represented by OMG’s (Object management Group) solution for system abstraction, modelling, development, and reuse—Model Driven Architecture (MDA) (OMG Model Driven Architecture 2012). The key component of system modelling, which underlies the principles of MDA—Unified Modelling Language (UML)—is a widely accepted standard for modelling and designing different types of systems and is used to define several kinds of diagrams, their elements and notation (OMG Unified Modelling Language 2012).

The MDA models can be formally expressed by any sort of modelling language; however UML has been the dominant choice. The main goal of MDA is to provide the ability of automated transformations from platform independent models into platform-specific source code. Thus the models in MDA can have two different forms. The first form of models is the models that are independent of the operating platform. These types of models are called Platform Independent Models (PIM).

PIMs are abstract models that do not directly map to a specific environment. In order to perform the PIMs, Platform Specific Models (PSM) should be created. For instance the model of CI interdependencies expressed in UML and created during the study (described in Section IV of the paper) using StarUML tool (StarUML 2012) is platform independent and can be classified as a PIM. However to be able to create a real simulation, an agent based tool should be selected to apply it for model simulation. The PIM then should be transformed to a PSM to make it executable. Thereby the idea of problem domain abstraction from programming details and set of models proposed by MDA is borrowed for the analysis and implementation of risk level assessment for critical infrastructure.

4. WATER SERVICE PROVIDER CASE STUDY

In order to show the feasibility of the methodology a reference scenario is applied in this section, the UML use case diagram is created and the appropriate object interaction expressed in terms of the UML sequence diagram is summarized in the UML class diagram.

4.1. Situation Description

The reference scenario is composed of a high level representation of water utility (Talsi Water), which presents interdependencies with energy provider (Latvenergo CI) and a telecommunication provider (GSM Operator CI). This scenario is demonstrated as an example for validating the risk based methodology. A more complex and realistic representation is not possible due to the lack of the data and this work space constraint.

The risk analysis of Talsi Water CI has identified the internal service interdependencies of Water CI, as well as interdependencies between the Talsi Water CIs, Latvenergo and GSM Operator's CIs (see Fig. 2). Furthermore Fig. 3 shows how each service is composed of components needed to provide the service.

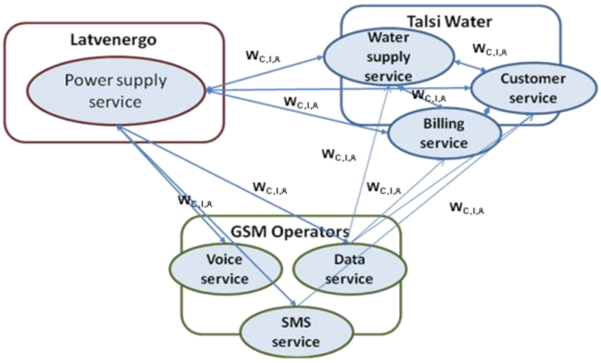


Figure 2: Interdependencies Between Services and Services Providers

As it is shown in Fig. 2, Talsi Water CI provides water supply, billing and customer care services. Water supply services utilize infrastructure components, for example, water supply service is based on water pumps, SCADA for water supply management, water meters and sensors – transmitters, data transmission gateways and data centre equipment (servers, data bases etc.) (Zabasta, Kunicina, Chaiko, and Ribickis, 2011). Data transmission gateway infrastructure relies completely on GPRS service provider. The part of the infrastructure components is shared among services, for example, data bases and servers.

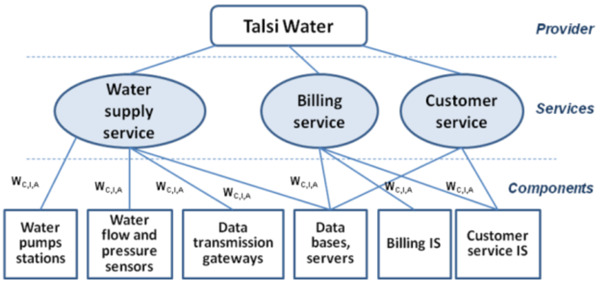


Figure 3: Talsi Water Services Decomposition

To simplify the example, it is assumed that the main infrastructure or GSM operator at reviewed territory consists of the base stations, which enable data traffic and SMS services for water supplier. It is assumed that the data transmission (GPRS) service and the GSM service would not be able to provide the service without power supply services (base station batteries enable back up for a few hours).

4.2. Interdependencies modelling with UML

In order to create the UML model of interdependent CI we apply StarUML, an open source UML tool, licensed under General Public License (GPL).

Use cases. As an example of the UML use case diagram, showed in Fig.4, let us consider the risk level assessment of integrated water supply service, which is influenced by data service of a telecommunication operator and power supply service of Latvenergo.

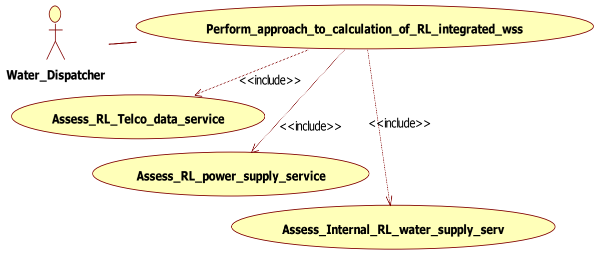

Water_Dispatcher
Perform_approach_to_calculation_of_RL_integrated_wss
<<include>>
<<include>>
<<include>>
Assess_RL_Telco_data_service
Assess_RL_power_supply_service
Assess_Internal_RL_water_supply_serv

Figure 4: Use Case Diagrams for The Risk Level Assessment

We use the actor symbol to represent the agent that activates the use case, which in our example is a water supply dispatcher, who wants to know the integrated risk level of water supply service.

The relation between the use case "*Perform approach_ to_ calculation_of_RL_integrated_wss*" and other use cases are represented by the relationship's stereotype «include» graphically depicted with a dashed arrowed line beginning at base use case and ending with an arrows pointing to the include use case.

Sequence diagrams. The detailed description of the interdependencies modelled through the use case diagrams is provided by one of the sequence diagrams in Fig. 5, which refines integrated risk level of water supply service. We have decided to use the sequence diagram because it focuses on the participants (agents, infrastructures and services) and links (interactions and interdependencies). Moreover the sequence diagram allows providing a clear description of the object interaction, message ordering, and the synchronous and asynchronous messages.

Furthermore the sequence diagrams describe in the similar way participants, interaction and interdependences in other use cases, but due to the lack of space we do not describe them in this work.

Class diagrams. Fig. 6 shows thirteen classes, where five of them represent water supply service with its services components, five classes represent power supply, one class data transmission services but one class starts and controls services risk level assessment process. The parameters of attributes and operations in each class have been omitted in the interest of figure clarity. One particular class, namely "Metrics", have been created in order to describe parameters of classes' attributes and classes' operations. The class has attributes "value", "weight" and "reference level" that are referred to the service parameters (availability, confidentiality and integrity). Creation of particular class makes sense since unified normalized parameters are applied to divergent CIs.

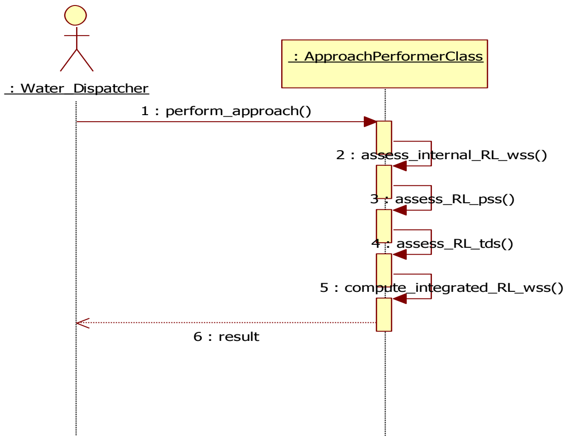


Figure 5: Calculating of Integrated Risk Level of Water Supply Service.

The ontology proposed in Fig. 6 was created in order to study CI interdependencies of the particular city, but can be readily adapted to other cases, taking into account the specifics of each city.

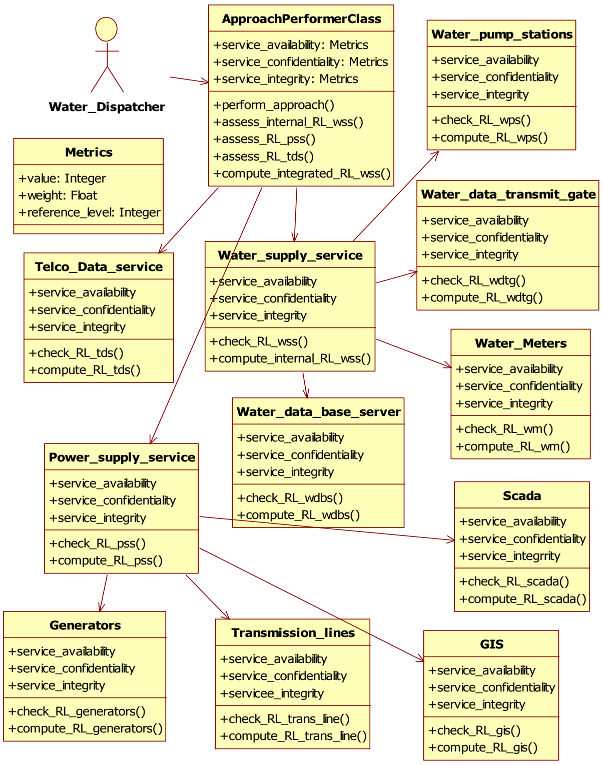


Figure 6: Interdependencies Class Diagram.

5. DISCUSSIONS AND FUTURE WORK

The four modelling steps are described in this work, they are service components assurance and risk assessment, measurement aggregation, services interdependencies linking and CI interdependencies modelling using UML. In this work we proved the hypothesis to abstract and to decompose services to a small set of common parameters; therefore three parameters were chosen to evaluate the state of services of different CI (confidentiality, integrity and availability), which are widely used for evaluation of systems security. The main advantage is that the model is easily extensible for including additional parameters and is ubiquitous for heterogeneous CI.

Another benefit of the CI security model for businesses is the ability to compare different types of infrastructure using common risk related parameters. A common set of parameters makes it easier to interpret the information received from dependent CIs or CI services.

The approach enabling critical information sharing among service providers allocated in neighbourhood looks quite attractive, because it helps to CI owners to make more qualified decisions and to plan risk mitigation actions. Moreover, the question is how to encourage service providers to elaborate, refine and issue critical information to other CI owner.

In this paper authors use the modelling notation offered by UML and the idea of information abstraction in models, defined at different levels of abstraction proposed by the MDA approach. We recognize that the used notational conventions bring about a better understanding and a clearer picture of the CI internal arrangement and external interdependencies.

An example of dependences of water supply and telecommunication services from the outages happened in power greed is described aiming to study CI interdependencies of the particular city; furthermore the ontology proposed in this work can be readily adapted to other cases, taking into account the specifics of each city.

One of the approach limitations is necessity to involve experts for weights definition; therefore future work should focus on enhancing weights definition on the functional model, transformation static into dynamic weights making the model less dependent from expert knowledge; looking for the methods for on-line monitoring of CI and mutual alerting of the critical levels of interdependent services. Future work also should focus on enhancing universal approach to services decomposition and measures aggregation for heterogeneous CI.

Another limitation is that simulation of critical infrastructures is not a task of this work; therefore to form a complete modelling and simulation cycle, we plan to transform PIM, developed in the research, into platform specific model. The intended PSM will be based on an agent based architecture because we need to get input from distributed systems such power supply systems, telecommunication networks and water distribution networks.

REFERENCES

Aubert, J., Schaberreiter, T., Incoul C. and Khadraoui D., 2010. Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures, *Proceedings of ESREL 2010*, pp.1-8, Rhodes, Greece, September 5-9. 5

Aubert, J.; Schaberreiter, T.; Incoul, C.; Khadraoui, D.; Gateau, B., 2010. Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures, ARES '10 International Conference on Availability, Reliability and Security, pp. 262-267, Feb. 15 – 18, 2010, Krakow, Poland. 8

Bagheri E., Ghorbani A., Towards an MDA-Oriented UML Profile for Critical Infrastructure Modelling, *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services, PST 2006*, pp.1-1212, Oct.30 – Nov. 1, Ontario, Canada. 11

Casalicchio, M. and Galli, E., 2008. Metrics for Quantifying Interdependencies, *Proceedings of Second IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, pp. 1-8, George Mason University, Arlington, VA, USA, March 2008. 2

ISO 15408-1:2009, 2009. Part 1: Introduction and general model, Information technology Security techniques, Evaluation criteria for IT security, pp.1-72, ISO, Geneva, Switzerland. 13

ISO/IEC 27001:2005, 2005. Information technology, Security techniques, Information security management systems – Requirements, pp.1-188, ISO, Geneva, Switzerland 14

Lin J., Sedigh S., and Miller A., 2010. Modelling Cyber-Physical Systems with Semantic Agents, *34th Annual IEEE Computer Software and Applications Conference Workshops (COMPSACW 2010)*, pp.13-18, July 19- 23, Seoul, Korea. 12

OMG Model Driven Architecture, [Online]. Available from: http://www.omg.org/mda [Accessed: March 21, 2012] 15

OMG Unified Modelling Language, [Online]. Available from: http://www.uml.org [Accessed: March. 21 2012]. 16

Refined interdependency metrics and indexes for risk prediction formulation, 2010. Project D3.1.2. *Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures* (MICIE), FP7, STREP, 22/06/2010, pp.1-186. 3

Rinaldi, S.M., 2005. Modelling and simulating critical infrastructures and their interdependencies. *Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04) - Track 2,* pp.1-8, Washington, 4.1. IEEE Computer Society. 6

Setolaa, R., De Porcellinise, S., Sforna M., 2009. Critical infrastructure dependency assessment using the input– output inoperability model, *International Journal of Critical Infrastructure Protection*, 2, pp. 170 – 178. 1

Schaberreiter T., Bonhomme C., Aubert J., Incoul C. and Khadraoui D., 2010. Support tool development for real-time risk prediction in interdependent critical infrastructures service, International *Workshop on Risk and Trust in Extended Enterprises (RTEE'2010*), pp. 1- 8, San Jose, California – USA, November 1-4, 2010. 7

StarUML - The Open Source UML/MDA Platform, [Online]. Available from: http://staruml.sourceforge.net/en/download.php [Accessed: March 21, 2012] 17

Zabasta A., Kunicina N., Chaiko Y., and Ribickis L., 2011, Automatic Meters Reading for Water Distribution Network in Talsi City, *in proceeding of EUROCON 2011*, 27-29 April 2011, pp. 1-6, Lisbon, Portugal. 20

Zabasta A., Kunicina N., 2012. Approach for Monitoring and Measurement of Interdependent Services in Critical Infrastructures, *Proceeding of the 11th International Symposium, Faculty of Power Engendering, Tallinn University of Technology*, pp.51-56, Pärnu, Estonia. 10

CAX METHODOLOGY FOR CIVIL PROTECTION OPERATIONS AND CIVIL MILITARY CO OPERATION

Konstantinos Tsiakalos, MSc Statistics & Op. Research

University of Genoa

kotsiak@otenet.gr

ABSTRACT

The main idea of this paper is to prove that Computer Assisted Exercises methodology, based on modeling and simulation for military operations mainly, can be used for civil protection operations and civil – military co operation.

Beginning with a general overview of the fundamentals of CAX and continuing with a proposal for reforming the methodology in a more appropriate way for civil protection operations, there is a first contact and understanding of it. CAX can become the important tool for creating “reactions” for national, multinational and international organizations in order to face unexpected actions that may harm the security, health and even life of civilians.

By playing scenarios representing rational or irrational situations threatening civilians life in general, all agencies responsible for civilian protection can be trained in a realistic environment and test their capabilities. Matters of training costs and exercise budgets are also discussed here as it is obvious that the usage of CAX methodology can eliminate both.

Furthermore, the presentation of game theory models for improving all phases of the CAX methodology is providing an innovative idea which is maximizing the benefits of a CAX and produces a secure path for studying the results of it.

Key words: Computer Assisted Exercise, Civil Protection Operations, Civil – Military Co operation, Game Theory Models.

1. INTRODUCTION

During the last twenty years, mostly in NATO nations the usage of Computer Assisted Exercise (CAX) methodology has become an important tool for operational staffs and decision makers in general. This methodology based on modeling and simulation, especially discrete events simulation, has been developed very fast in addition to simulation models providing results through stochastic processes. Simulation models for military purposes, such as Joint Theatre Level Simulation (JTLS) or Joint Conflict and Tactical Simulation (JCATS), Marcus, etc., or even more simulation platforms and mathematical models used for military simulations have became extremely “realistic”, simulating accurately military operations of different levels and services. Exercises in NATO and NATO nations have proven that CAX methodology is capable of achieving two very important objectives:

1. Reduce the training budget and at the same time provide a more realistic environment for the training audience.
2. Introduce modeling and simulation to military people in a way which has given them an alternative view for multilevel - multipurpose operations, mainly large scale operations in unknown environments with hostile populations.

As a matter of fact, the results of CAX methodology are impressive in the military area of interest. The result of this success brought up a vital question: Can the CAX methodology used for other than military operations? The answer is absolutely yes. In this paper, it will be presented how CAX methodology can be used for civil protection operations and civil – military cooperation purposes. Also, a new approach for CAX methodology is going to be described for all phases of a CAX and particularly the introduction of a new phase and the way that this new phase can provide to decision makers, think tanks and staffs, solutions to their real life scenarios and situations.

It is of great importance to understand the concept of the CAX methodology and this is the reason for giving first of all some definitions and descriptions of the CAX methodology that NATO uses. At the same time, it is necessary to refer to the role of modeling and simulation to CAX methodology. Inserting game theory tools and mathematical models of conflict and co operation in CAX methodology, is extremely innovative and it may be a challenging beginning for producing a more effective and efficient approach. The results of such an approach will surly give decision makers, think tanks, staffs and organizations managers the capability of “translating” the conclusions of simulation to acting plans without waste of time and in a costless way.

It has to be mentioned that there are not many available resources referring to CAX methodology and many of the CAX results are of high classification. This fact is slurred over by the author's experience in the area due to his military background, as he has contacted more than 120 national and international CAX's. The improvement of CAX methodology and its usage for civil protection operations and civil – military co operation needs to be relied on three pillars:

1. Operational research tools.
2. Multilevel, multipurpose simulation models.
3. Accurate and secure simulation results analysis.

Finally, for every one of the above pillars there is a certain level of importance which is going to be discussed separately for everyone of them and at the same time the role of each of them needs to be clarified in order to have a full picture of how the CAX procedures will be formed efficiently for civil operations and civil – military co operation simulation.

2. COMPUTER ASSISTED EXERCISES (CAX)

Application of simulation models in CAX methodology is representing an educational method, which is dynamically introducing operational conditions of real systems in synthetic environment. Dynamic training system is consisting of digital terrain, environment and equipment allowing to the exercise participants to gain new knowledge, skills and behavior. Each CAX is also a research method, because is fulfilling a few conditions for that, for example:

1. Novelty of the problem.
2. Importance and applicability of solutions for the practice.
3. Level of interest in problem solving processes.
4. Available equipment and other research conditions.
5. Actuality of research results.
6. Possibility to find solution for the decision making problems by research.

Through the process of CAX we are undoubtedly optimizing current staff procedures and decision making processes in synchronization with all other stakeholders in the area of responsibility.

In order to properly apply above mentioned training methodology, it is of utmost importance to understand the potential needs of the country, organization, or in any case the "clients'" needs. Ultimate goal is to provide training conditions for audience in order to achieve training objectives. That will prepare them for the real world crisis decision making process on strategic, operational or tactical level.

The main issue here is the method or the process that we need to use for understanding the needs of the final "client" or even more the capability of the CAX organizational structure to produce certain results based on discrete and explicit requirements.

If for example the requirement is to plan, prepare and execute a CAX based on an earthquake or more generally speaking a natural disaster scenario involving national, multinational and international organizations and agencies, we need to describe - model in a simulation system the capabilities, structures, doctrines, means and possible reactions of all entities that will have a role in this scenario.

These entities will be the units of countries that will take action to save civilians (army, police, fire brigades, special forces, etc.), the organizations that will control the operations, the C2 systems, the facilities that will be used and every other autonomous and partially described forces that can affect the situations or the events of the scenario.

Definition 1: A CAX is usually defined as a type of Synthetic Exercise (SYNEX) where forces are generated, moved and managed in a simulation environment based on the commands coming from the exercise participants (Cayirci – Marincic 2009).

CAX is above all a methodology and a way to provide results based on simulation. Decision makers, think tanks, staffs and command and control teams are not supposed to follow the row of simulation but is more than enough for them to understand that processes and procedures are close to their directives and doctrines.

As a matter of fact, CAX can provide wide area training for different kind of operations and levels. Therefore, CAX support is often thought limited to installing and running a military constructive simulation during a CPX (Command Post Exercise). In this perception CAX support is to replace or to help Response Cells, Higher Level Commands (HICON), Lower Level Commands (LOCON) to find out the possible outcomes of the decisions or requests coming from the Training Audience (TA) by running a set of stochastic processes. However, CAX is in essence a CPX where electronic means are used:

1. To immerse the TA in an environment as realistic as possible.
2. To help the exercise planning group (EPG) and the exercise control (EXCON) staff for controlling the exercise process (EP) so that it achieves the objectives as effectively as possible.

In the execution phase of a CAX, most of times we use discrete events dynamic simulation to represent complex operations. Constructive simulation systems are commonly used to simulate those operations. They can interact with the Training Audience through the CAX experts and in the very high resolution analysis level (tactical or operational, depending on the kind of

operations) visualization is also used to represent specific events of a structured scenario or activities that guide the Training Audience to certain actions.
The simulation cycle is followed in order to express the interaction between Training Audience and simulation system. CAX experts are receiving orders from Training Audience and C2 systems, they put them to the simulation system and they are feeding back the Training Audience with the results of simulation, as shown in the following picture:

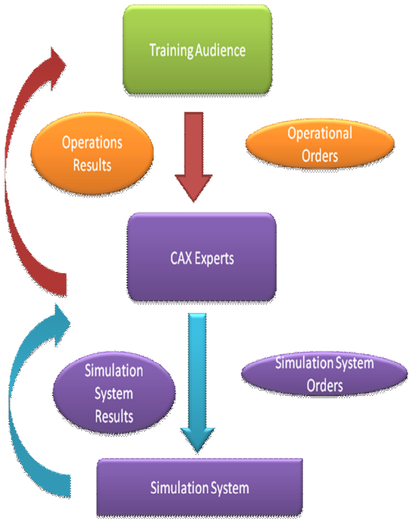


Figure 1: From the Training Audience to the Simulation system

CAX is ensuring high quality of individual and collective training on decision making processes on tactical, operational and strategic level (Cayirci – Marincic 2009).

2.1. Typical NATO CAX Architecture

There is a typical NATO architecture and methodology followed by a serious number of countries, agencies and organizations, based on NATO's doctrine *Bi 75-3*.

Some vital meanings and issues used in this methodology have to be mentioned and defined, through which the whole structure of a CAX will be more easily understood.

A CAX in NATO needs about 12 – 18 months of planning and preparation and usually takes about 10 – 15 days for its execution phase. After Action Review and Lessons Learned can be referred as the last phase of a CAX.

NATO CAX methodology consists of the following phases:

1. Planning Phase
2. Preparation Phase
3. Execution Phase
4. After Action Review Phase

Before the Execution Phase a number of conferences is being held for coordination purposes and these are the following:

- Initial Planning Conference (IPC)
- Main Planning Conference (MPC)
- Final Co ordination Conference (FCC)

During the preparation a number of conferences is taking place basically for commanding and controlling the project. There are two main architectures for a CAX:

- Distributed CAX, where all the participants are sited in their natural positions.
- Non distributed CAX where all participants are in the same place.

In both cases we can have *distributed* or *non distributed simulation*, which depends basically in the type of simulation model(s) that is (are) going to be used in the CAX. The CAX architecture is not affecting the type of simulation (distributed or not). In both cases, the architecture fundamentals are shown in the next figure:

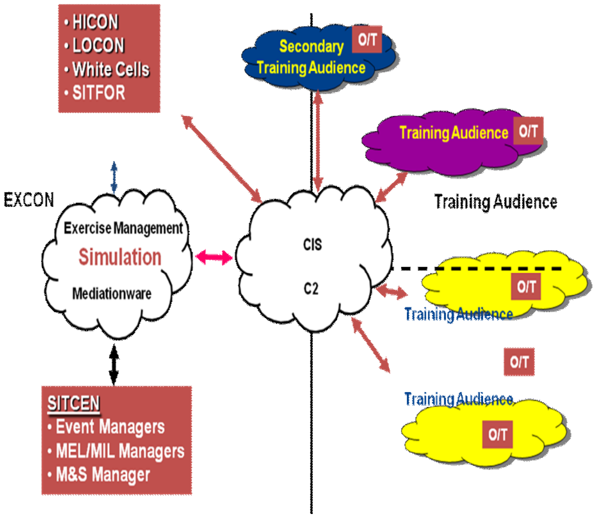


Figure 2: Architecture for Distributed CAX

The above figure describes the architecture for distributed CAX's as it fits perfectly with NATO's requirements and mostly with NATO's operational needs (Cayirci and Marincic, 2009).

Training Audience can be:

- Cross leveled, which means that it is coming from same level of command but from different services.

- Multi leveled, meaning that it is coming from the same service but different command levels
- Multi – Cross leveled, both from different services and different command levels.

Training Audience represents friendly side(s) and the opposing forces are usually called Situational Forces (SITFOR). Other organizations or agencies, playing important or less important roles in the scenario are represented as Gray Cells or White Cells.

Response Cells (RC) are the representations of higher and lower commands of friendly side(s). In the next figure there is a typical structure of a RC:

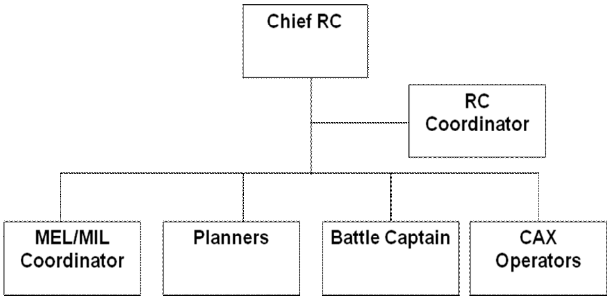


Figure 3: Typical Structure of a RC

Battle Captain's role is to translate Training Audience with CAX Operators and transport simulation results to operational people.

Main Events List / Main Incidents List Coordinator is responsible for checking if simulation follows the scenario major events and planning.

Another important element of the CAX methodology is the Exercise Centre which controls the CAX during the execution phase and at the same time has the full responsibility for running the simulation. EXCEN has the following roles:

1. Is connecting, in a way, simulation personnel with operational personnel.
2. Assists operational staff to understand the concept of simulation for given scenarios.

In other words, EXCEN is the most vital element of a CAX procedure and the main factor that can guarantee the success of the CAX.

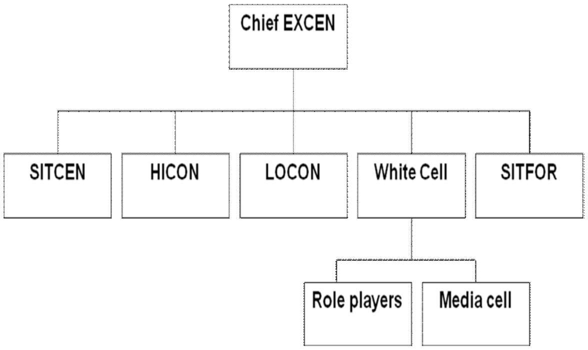


Figure 4: Exercise Centre

After concluding the execution phase of a CAX there is always an After Action Review procedure concerning mainly the analysts and the planners of the exercise. In many cases, participants in the After Action Review procedure are the Training Audience (Primary and Secondary), depending on the level of the exercise, the objectives and special features of it. The final products of the above procedure are lessons learned and lessons indentified. Both of them are not coming directly from the simulation results but they are analysis conclusions and many times even research based on some of the simulation results.

It has also to be mentioned that C2 systems, networking, non simulation software and informatics tools are used to support a CAX during the execution phase.

2.2. The SEESIM CAX

In many cases, like the South Eastern Europe Simulation (SEESIM) project, held by the South Eastern Europe Defense Ministerial (SEDM), the CAX methods are being followed in another way, trying to simulate the procedures and processes of the military – civilian organizations- agencies reactions in a multinational environment. The structure of SEESIM04 is shown in the figure:

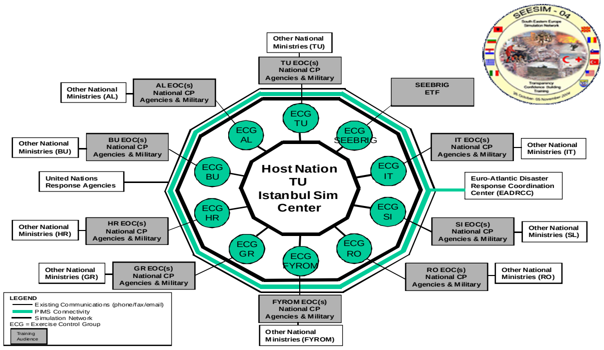

SEESIM - 04
South Eastern Europe Simulation Network
Transparency Confidence Building Training
25 October - 05 November 2004
Other National Ministries (TU)
TU EOC(s) National CP Agencies & Military
SEEBRIG ETF
Other National Ministries (AL)
AL EOC(s) National CP Agencies & Military
Other National Ministries (BU)
BU EOC(s) National CP Agencies & Military
United Nations Response Agencies
Other National Ministries (HR)
HR EOC(s) National CP Agencies & Military
Other National Ministries (GR)
GR EOC(s) National CP Agencies & Military
IT EOC(s) National CP Agencies & Military
Other National Ministries (IT)
Euro-Atlantic Disaster Response Coordination Center (EADRCC)
SI EOC(s) National CP Agencies & Military
Other National Ministries (SL)
RO EOC(s) National CP Agencies & Military
Other National Ministries (RO)
FYROM EOC(s) National CP Agencies & Military
Other National Ministries (FYROM)
ECG TU
ECG AL
ECG SEEBRIG
ECG BU
ECG IT
ECG HR
ECG SI
ECG GR
ECG RO
ECG FYROM
Host Nation TU Istanbul Sim Center
LEGEND
Existing Communications (phone/fax/email)
PIMS Connectivity
Simulation Network
ECG = Exercise Control Group
Training Audience

Figure 5: SEESIM 04 Structure

As one of the participants was the South East Europe Brigade (SEEBRIG), SEESIM is the most suitable example of a multinational CAX for civil protection and civil military co operation. The scenarios used for simulation were describing a wide range of destructions (coming from nature's or terrorists' "actions") and events affecting mainly civilians and critical national infrastructure. The main objectives of this CAX were:

- Practice and improve standard procedures for training the participants' national Emergency operational Centers (EOC) and SEEBRIG HQ in regional information management, communication flow, and coordination of humanitarian assistance, consequence management and disaster response operations.
- Promote national and regional preparedness for civil and military agencies and SEEBRIG in order to respond effectively in terrorist activities.
- Practice timely information exchange between national and regional emergency centers for quick counteracting terrorist, Chemical, Biological, Radiological and High Explosive proliferation activities or mitigate effects of disasters.

For achieving the above objectives the SEESIM CAX's 2002 till 2010 methodology differ in some points from NATO's methodology, mainly because of the differences of national EOC's and the interference of non military agencies. A standard CAX methodology was followed, most of times taking in consideration the special features, relations and restrictions of the South East European countries.

Some of the negative conclusions that SEESIM project experienced are the following:

- CAX methodology can be surly used for civil protection operations and civil – military co operation.
- Even an inter ministerial co operation in one country has to be very carefully and detailed described in order to be simulated in the most realistic way.
- Time limitations in all phases were not followed and reaction time during simulation from agencies and / or organizations were too long.
- Data given from participants (nations) for building simulation models databases were changing till the last moment.
- Working Groups managers couldn't easily balance the differences between nations and philosophy of exercises.
- Simulation process was not running properly and a great number of mistakes happened due to untrained personnel.
- After Action Review process gave some general and uncertain results mainly because the simulation was not running properly and analysts couldn't understand nations' activities for facing specific scenario problems.

The SEESIM project was supported by a number of CAX experts and advisors coming from US JFCOM (which was later transformed in JCW). The idea of simulating physical disasters and asymmetric threats and the reactions of agencies and organizations of Southeast Europe nations, brought up a vital question: Was CAX methodology used by US JFCOM proper for such a project? After five exercises we can certainly give an answer: The above conclusions showed, up to a point, that it had some kind of success but the organizers did not get what they expected. As a result SEESIM 12 will be supported from NATO / JWC, which means that a methodology closest to NATO's one may be more proper.

Based in this methodology, in the following paragraphs it will be presented a more convenient and suitable philosophy for CAX's dealing with civil protection operation and civil military co operation.

3. FUNTEMENTALS OF CAX METHODOLOGY FOR CIVIL – PROTECTION OPERATIONS AND CIVIL – MILITARY CO OPERATION

In many cases we have seen in the past natural disasters, humanitarian crisis, violence in metropolitan cities and even more disasters coming from unexpected recourses affecting the life of civilians and bringing serious problems in the rest of the world. "Katrina", the Thailand tsunami, Somalia, violent behavior even in schools in US, can affect lives and people in a very short time limit. To improve our reaction, is absolutely necessary to find the "optimal paths" and the proper models for "guessing" what may happen and how we can manage it.

First of all the need a wider and more comprehensive definition of CAX are obvious that it is necessary, mainly for two reasons:

- To include the simulation cycle during the execution phase of a CAX
- To express the expectations / outcomes from a CAX.

We will proceed in the following definition:

Definition 2: A Computer Assisted Exercise is a synthetic exercise where electronic means are used to simulate scenarios, processes and procedures of all kind and levels of operations, in complex environments. Simulation is executed by experts who receive operational orders from the Training Audience; they interact with simulation models and feeding back the Training Audience with the results of simulation. The products - objectives of a CAX are: realistic training for the Training Audience and control, evaluation and administration of operations for the Exercise Control Group and Operational Planners.

In a perspective, the usage of CAX methodology for civil protection operations and civil military co operation requires:

1. Careful and detailed preparation.
2. Time Synchronization for all levels and all kinds of operations.
3. Applicability of simulation models.
4. Special analysis tools for building scenarios, including maps, statistics for natural phenomena, executive planning, terrorist and civilian “behaviors”, mass and social media role and military involvement in civilian issues.
5. Support tools for scenario(s) and exercise management.
6. Interoperability of simulation systems for multilevel –multipurpose simulation.
7. Simple and clear scenario(s).
8. Experienced and expert operational and technical personnel.

To meet these requirements some vital changes have to be made in the whole philosophy of the CAX methodology.

Constructive simulation has to be used for producing more realistic results and also entities to be more detailed described. The need of multilevel – multipurpose simulation is also an important problem. This can be solved by using models’ federations (FOM) which are communicating each other through High Level Architecture (HLA). Such a federation is NATO Training Federation, using Joint Theater Level Simulation (JTLS), Joint and Tactical Simulation (JCATS) and Visual Battle Space 2 (VBS2). In any case, HLA can offer us the capability of interoperable models which can simulate in a synchronized mode different kinds and levels of operations.

It is also important to insert the procedure of visualization for every level and kind of operation. Visualization assists operational people to understand better the environment of simulation and provides them with the capability of having pictures of what is going to happen in front of their eyes, which is easier to accept.

There is no need to have visualization process synchronized with simulation. Based on the results of simulation we can use other models to show “what happened”. The critical idea here is to present to the Training Audience in the most realistic way the results of their reactions.

Last but not least, the absolute need of giving operational people real significant services, leads to a different approach regarding the After Action Review phase. Till now, everybody was happy with Lessons Learned and Lessons Indentified. But is this what a decision maker or a staff manager needs? The answer is absolutely no. After all, simulation provides a lot more than lessons. Simulation can be a small window to the future and is capable to reveal what may happen under given conditions and circumstances.

Based on this, by using proper tools, such as Game Theory models and Dynamic Programming, simulation’s results can be further analyzed and extract solutions and planning tips for CAX planners.

By using Game Theory models of conflict and co operation there are several problems that can be solved. One of the most important is to reduce casualties, meaning that human lives can be saved by “building’ a rational or irrational game between the “enemy” (that even nature can be) and friendly side(s). The outcomes of a realistic simulation may consist the parameters of the game(s) and what cannot be simulated can be introduced as the restriction(s) of the game(s).

On the other hand, dynamic programming is a mathematical tool which is solving a great number of problems regarding optimal processes. Linear Decision Making is offering to decision makers the capability to choose the optimal action between a numbers of proposed actions. By simulating a single event several times we can build a linear decision making problem and provide the decision maker with the optimal solution.

We can emphasize in the following conclusions:

1. CAX products must be <u>proposals / solutions,</u> which have been studied during and after simulation.
2. Decision makers can use those proposals immediately and without uncertainties or doubts for their planning and real life activities.
3. These proposals / solutions are the results of mathematical processes based on operational research tools (f.e. dynamic programming and game theory) which prove that they are the optimal for given scenarios.

3.1. A New CAX Model for Civil Protection Operations and Military Civilian Co Operation

In this paragraph it will be introduced a model of a new CAX model suitable for civil protection operations and civilian military co operation, Our basis for this model will be the NATO CAX methodology as described in NATO / ACT Doctrine *Bi 7-53 2007* and the experience of the SEESIM CAX. Additionally, some major changes regarding the After Action Review and the Lessons Learned phases will be included in order to optimize the results and conclusions of a CAX.

The first parameter that differs is that the proposed CAX model is treated as a unique project consisting of several different tasks which are undertaken by Task Managers, who are responsible for Task Groups. The number of the Task Groups can be different in every

CAX. The whole project is running divided in certain time phases and has to follow a complete plan and prefixed timelines and milestones. Tasks are assigned in CAX Task Managers and the whole project is assigned to a CAX Project Manager, as shown in the following figure 6

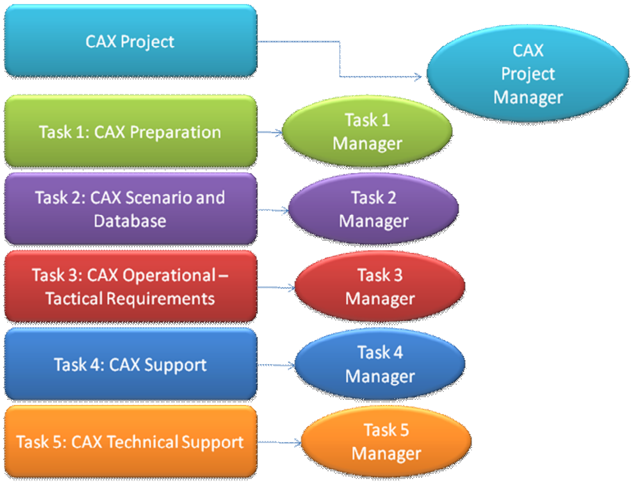


Figure 6: the CAX project

A second major change is concerning the phases of a CAX. These phases are basically time phases, in which tasks and sub tasks have to be concluded, based on a sequence of related activities. Also, there is a difference in the last phase which includes proposals, plans and solutions instead of After Action Review and Lessons Learned. These five discrete time periods – phases are:

1. Exercise Project Planning (1 -2 months).
2. Exercise Organization Procedures (3 – 5 months).
3. Exercise Execution (10 – 15 days).
4. Exercise Reports (2 -3 days).
5. Proposals – Plans – Solutions (10 – 15 days).

In every Task Group there are CAX experts who assist operational people in understanding the CAX features and special characteristics. By this way there is a significant time profit which leads to fewer costs. The Exercise Planning task has a main target: To define the training, exercise and simulation objectives. The final outcome of this task is the Exercise Plan (EXPLAN). The important and innovative intervention here is that in the EXPLAN must be mentioned time limits and milestones for the whole project, including and the after execution phases. Task Groups and Managers have to follow closely these time limits and millstones and deliver to the CAX Manager their work in the prearranged dates.

As shown, the preparation time of a CAX is limited to 4 -7 months, depending mainly on the following parameters:

1. The number of participants and the level of operations. Usually, tactical operations CAX needs less preparation time.
2. If the CAX involves international or multinational agencies and organizations. Multinational or international agencies need more time for coordination.
3. The entities analysis and scenario(s) length. Let's take an example: For building a realistic data base, coming from a 10 days earthquake or floods scenario, involving f.e. five nations and their Emergency Operations Centers (EOC), we may need more than 650 entities to describe the basic structure of operational, support units and facilities. This number is the average number of units used in SEESIM exercises for building JTLS database (units and targets).

The number of participants has to be defined by using an optimization process, which limits the personnel to the absolutely necessary. This leads to lower costs during the preparation of a CAX.

The optimization problem is described as follows: Let P the needed personnel for the preparation phases of a CAX, where $P = \sum_{i}^{k} p_i$ and p_i is defined as the needed personnel of the Task Group i. Every Task Group consists from different kind of personnel f.e. operational officers, technicians, CAX experts, etc.This can be represented as $p_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{ik}x_m$, where $x_1, x_2, \ldots, x_m$ are the different kinds of personnel and $a_{i1}, a_{i2}, \ldots, a_{ik}$ are the multipliers for every kind of personnel. Defining the available personnel for every Task Group as v_i there must be $p_i \le v_i$. In this case the optimization problem is to minimize P. By constructing an objective function taking in consideration the CAX requirements we solve the problem using the Simplex algorithm.

Scenario and database building in a CAX preparation is one of the most important elements of it. The process of scenario building has the following stages:

- Stage 1: A step by step analysis of the exercise, training and simulation objectives leading to a set of scenario requirements.
- Stage 2: Scenario(s) scripting where discrete events are described and connected to scenario requirements as given from Stage 1. After scripting every event is analyzed in a number of incidents and

every incident in actions and injections. It is necessary to build a time schedule for coordination purposes.

- Stage 3: As an outcome of Stage 2, there is a full plan of structured entities with discrete roles in simulation. This plan is given to technical personnel (experts in simulation models) of the proper Task Group who proceeds to the following steps:
  - Model the entities
  - Building of the database in the simulation model
  - Verification
  - Validation
  - Testing and evaluation of the database
  - Documentation
  - Test scenario(s) and present to Exercise Planners.

For the civil protection operations and military – civilian co operation we need to define a number of parameters to specify the scenario(s) requirements. The most significant of them are:

- Time limitations (T_l) and reaction time (T_r, by real world statistics) of the simulated entities (units, services, etc.).
- Command structure and logistics structure of all entities.
- Means and manpower of the entities.
- Geostrategic environment and international restrictions and affairs of the involved participants.
- Interrelations between military and civilian organizations and agencies.
- Discrete roles of military and civilian organization for every kind of operation.
- Support costs (s_c).
- Transportation costs (TR_c).
- Information exchange systems (C2, C3, C4I).
- Nations, agencies or / and organizations capabilities and experience in civil protection operations.

In the preparation phases (Planning and Organization procedures), there specific aspects that have to be taken in serious consideration in order to provide solutions for the execution phase. These aspects are grouped in two major categories, analyzed as follows:

1. Technical Capabilities:

- IT systems that will be used and their capabilities.
- Personnel's technical skills, experience and capabilities.
- Type of reports of the simulation models, results computing, recovery processes, communications between Training Audience and other CAX elements during execution phase.
- Data extracting and processing capabilities.

2. Operational (Tactical) Planning :

- The level of operations that are going to be simulated and operations' complexity.
- Extension and analysis level of information needed for modeling and simulation. Constructive simulation models and stochastic simulation usually need a great amount of information and deep analysis of entities' attributes.
- Security restrictions and measures that can affect the realism of simulation. As a comment here we have to stress that the level of realism in a simulation is a function of several variables and it is not depending only to the level of details described in the modeling process.

During the execution phase, EXCON, RC and mainly SITCEN will suffer major changes. The main reason for this is to simplify the procedures. Another reason is that many times nature is involved as the "enemy" in SITFOR and also the "translator" between simulation and operational people has to be a CAX Expert with operational background. From this point of view, the people involved in RC's must have a detailed training in CAX issues. As a result of the above the following figure is showing a proposed structure for RC:

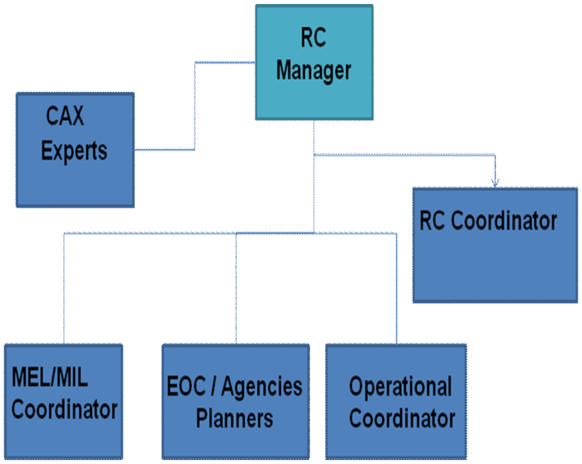


Figure 7:Structure of a RC

It has to be mentioned that the operational Coordinator will be the connector between CAX Experts and operational personnel and at the same time he will transfer operational orders from TA to CAX Experts.

Finally, there is a vital discussion here about introducing some mathematical models and methodologies that can provide more secure results and take less preparation time. Lets us see how Game Theory models may be a useful tool for all phases of a CAX. In the next entity it will be examined the capability of Oceanic Games and especially Voting Games, to change processes and procedures of a CAX in order to achieve two basic targets: Exercises cost reduction and optimal usage of simulation conclusions.

4. GAME THEORY MODELS SUITABLE FOR CAX PROCEDURES

Game Theory is a branch of Operational Research which has been an extremely useful tool for a various range of applications, especially in the field of financial services. By using statistics, dynamic and linear programming and sometimes "difficult" mathematics has produced quite a success solving problems and giving solutions in complex problems.

A very special part in Game Theory is the Oceanic Games, which are used for solving problems related to decision making processes. A subset of Oceanic Games are the Voting Games, used to describe games in voting systems, political and financial organizations decision making procedures and how power is divided among the independent parts of such organizations.

The tool which these games are employing is Power Indexes. Power Indexes are mathematical modules in order to measure the power of every discrete "player" in a game. The most common used are the Shapley – Shubik and Banzhaf power indexes.

More analytical, a voting arrangement in which voters may control unequal number of votes and decisions are made by forming coalitions with the total of votes equal or in access of an agreed upon quota is called a weighted voting system. The usual notation is $[q: w_1, w_2, ..., w_n]$, where *n* is the number of voters; w_1, *i = 1, ..., n,* is the number of votes controlled by the *i-th* voter, and *q* is the passing quota.

In the theory of weighted voting system it's customary to refer to voters as players.

F.e., in the system [5: 3, 2, 1], all decisions could be made by the two principal players (3 and 2 votes, respectively), while that last player (the one with the single vote) has no influence whatsoever on the decision process. It is then clear that having a vote does not endow its owner with any real power in making decisions. (The last player in this example is known as a dummy.)

Banzhaf's is one possible indicator of the relevance of a particular player. Shapley-Shubik's is another. In both cases, the power wielded by a player is determined by the number of coalitions in which his or her role is important. However, the two indices formalize the notions of coalition and importance in different ways.

Coalition is any (non-empty) combination of the players. A coalition is winning provided the cumulative vote of its members is equal to or greater than the quota. A coalition is losing if it's not winning. A player is called critical to a winning coalition, if his or her removal from the coalition renders it losing. Banzhaf's index of a player p is the ratio of the number of winning coalitions to which p is critical to the total number of times the players are critical.

A coalition is just a set of its elements. No order is specified in which the players enter the coalition. Not so with the sequential coalition, used to define the Shapley-Shubik index.

A sequential coalition of n players $p_1, p_2, ..., p_n$ is any permutation $p_{i1}, p_{i2}, ..., p_{in}$ of that set. An element p_{ik} is said to be pivotal to a (sequential) coalition $p_{i1}, p_{i2}, ..., p_{in}$ provided the (regular) coalition $p_{i1}, p_{i2}, ..., p_{ik-1}$ is losing, whereas the (regular) coalition $p_{i1}, p_{i2}, ..., p_{ik}$ is winning.

Assuming that the quota does not exceed the total number of votes, every sequential coalition has a unique pivotal element. Shapley-Shubik's index of power of a player p is the ratio of the number of sequential coalitions for which p is pivotal to the total number of sequential coalitions, which is always *n!*.

After describing the mathematical background, the research activity related to the CAX procedures is going to be following:

1. During the phase of CAX planning the building of a voting game where the objectives of a CAX (exercise, training and simulation) will be measured in order to decide the significance of them and also the "simulation behavior" of them. The meaning of the "simulation behavior", is essentially how much effort in different areas, we have to put during the simulation process, in order to achieve a specific objective under given restrictions. Actually, these restrictions can describe the level of realism of simulation.
2. The phase of the CAX organizing is the most vital. We have to be very careful and sure about the steps we have to undertake in order to "drive" the CAX according to the objectives given from the previous phase. In this case, we are building another voting game and by measuring the power of the different components of the CAX, we can justify the timetables, milestones, line of procedures, planning activities and finally the full Exercise Structure via the calculation of the important values of the CAX.
3. The execution phase of a CAX is going to roll on if our work during the organizing phase is productive. There are numerous elements that have to be measured for assisting us to achieve the Exercise, Training and Simulation Objectives. We can give the following examples:

- Force ratios for ground forces in specified geographical areas. Such ratios are combined with empirical knowledge to assess very rapidly what the trend of the exercise is and whether it is in line with the expected exercise flow. Should the actual trend deviate too much over time from the intended evolution, exercise directing staff may wish to capture the reasons for the deviation for after-action review purposes and may wish to introduce elements that may reduce the deviation without appearing to be artificial to the exercising headquarters.

- Attrition of high value assets for air and maritime forces. Given the many scarce resources that are employed in these forces and their potential to influence operations in a significant manner, any attrition needs to be reported and its causes identified. The directing staff must be able to make a timely assessment of the impact of the attrition on the course of the exercise and develop suitable courses of action from an exercise management perspective.
- Entities that represent civilian organizations, police, fire brigade, coastguard etc., are "fighting" against nature or against not recognizable enemies or even more against enemies without tactics and doctrines. In this case the kind of attrition is more or less following the ground units attrition rules for those entities that fighting in the ground and for all the others an attrition model that gives more probabilities to the "enemy".

Working exactly in the same way, building a voting game to calculate the important elements of every procedure and process and also to express in the most realistic way the results of simulation are providing a full description of the "behavior" of these elements under the restrictions of the simulation environment. How significant these restrictions can be, is measured by another voting game for calculating the power of specific data of this environment.

5. COST EFFECTIVENESS AND CONCLUSIONS

The vital targets by using CAX methodology for civil protection operations and civil – military co operation can be briefed as follows:

- Reduce the reaction time for civil protection operations and military – civilian co operation, which means fewer casualties in human lives.
- Reduce the costs of training, supporting and acting in civil protection operations and military – civilian co operation.

As a conclusion, we may say that by using CAX methodology we can surly achieve both the above targets, as it's already proved that this worked in the military area of interest. By accepting the fact that civil protection operation are not so complicated as military operations, especially in the operational and strategic level, it is obvious that by "tailoring" CAX methodology for civil protection operations we have good chances to succeed.

REFERENCES

Bertsekas D. (2007). Dynamic Programming and Optimal Control, Athena Scientific, Volume 2.

Cayirci E., Dusan M (2009). Computer Assisted Exercises, Willey.

Crichton, M. (2001). Training for Decision Making During Emergencies. Horizons of Psychology

Dusan M (2002). CAX as a Training Method, of the Peace Forces Components for the Peace operations. Ljubliana: Faculty of Social Science.

Dusan M., (2005). Simulation and Analysis for Peace Operations" Ljubliana: Faculty of Social Science, Dissertation.

Gibbons R., (1992). A Primer in Game Theory, Harvester.

IEEE Standard for Distributed Interactive Simulation Communication Services and Profiles, 1995, IEEE Ltd

Melolidakis K. (2009). Game Theory, Mathematical Models of Conflict and Cooperation, Athens, Sophia.

NATO Computer Assisted Exercise Doctrine Bi 75-3, Norfolk Allied Command Transformation, 2007

SEESIM Preparation Papers and Lessons Learned 2002, 2004, 2006,2008, 2010

AUTHORS BIOGRAPHY

Konstantinos Tsiakalos was born in Athens Greece in 1968. In September 1987 entered the Greek Military Academy and in June 1991 he graduated as Second Lieutenant of the Army Engineers.

In 1997 he graduated from the Greek Analysts and Programmers School and in 2002 he finished his Msc in Statistics and Op. Research from the mathematical Department of University of Athens. In 2012 he was accepted as Phd student in University of Genoa/Modeling and Simulation Department. In the Army he served from 2002 until 2012 in the Hellenic Modeling and Simulation Centre taking many responsibilities and duties and finally becoming director of the Centre for six months.

He has been awarded with all the medals and prizes for his rank and duties. He has also set the basis for the doctrines and directives for the CAX processes and procedures in the Hellenic Armed Forces General Staff during April 2011 till August 2011.

Furthermore, he proposed a full training system for CAX – Modeling and Simulation in August 2011 for the Hellenic Armed Forces General Staff. In January 2012 he retired from the Army as full Colonel of Research and Informatics. From February 2012 till now he is the CAX – Modeling and Simulation Department Manager of Miltech Hellas S.A., a defense industry company. The Department has already set some international co operations with organizations and countries worldwide. He participated in several national (more than 60) and international Computer Assisted Exercises and Experimentations.

Experimentation on CIMIC and PSYOPS Simulators

Agostino Bruzzone[a], Francesca Madeo [b], Claudia Frydman [c],
Simonluca Poggi [d], Marina Massei [e], Gregory Zacharewicz [f]

[a] DIME, University of Genoa - URL www.itim.unige.it
[b] Simulation Team - *URL* www.simulationteam.com
[c] LSIS Marseille - *URL* www.lsis.org
[d] MAST srl - *URL* www.mastsrl.eu
[e] Liophant Simulation - *URL* www.liophant.org
[f] IMS Bordeaux University - *URL* www.ims-bordeaux.fr

[a]agostino@itim.unige.it, [b] madeo@simulationteam.com, [c] Claudia.frydman@lsis.org,
[d] simonluca.poggi@mastsrl.eu, [e] massei@itim.unige.it, [f] gregory.zacharewicz@u-bordeaux1.fr

ABSTRACT

The research proposes a simulation model developed by the authors to support CIMIC (Civil- military cooperation) and PSYOPs (psychological operations) operational planning in complex scenarios (i.e. Afghanistan) characterized by crisis and conflicts.

The research is related to CAPRICORN R&D Project (CIMIC and Planning Research In Complex Operational Realistic Network), sponsored by EDA (European Defense Agency). The CAPRICORN model is based on a new generation of IA-CGF (Intelligent Agents for Computer Generated Forces) that is developed by the authors and is able to reproduce human factors as well as social and cultural aspects within the population. The authors provide the experimentation approach used to validate and test the model by strongly involving users and SME (Subject Matter Experts) and present the experimental analysis of results based on Design of Experiment techniques: MSpE (Mean Square pure Error) and sensitivity analysis.

1. INTRODUCTION

In the last decades, in countries such as Kosovo, Afghanistan or Iraq, characterized by conflicts and civil wars, after the pure coercive military actions, it is becoming necessary to face new post-conflict threats such as terrorism, insurgency or economic disruptions by engaging military forces in stability operations (Galula 1964; Chauvancy 2011). The main goal of this kind of operations is to recover social, economic and political conditions in these countries.

Therefore military defense is facing new issues and challenges and new activities are emerging such as Civil Military Cooperation (CIMIC) and Psychological Operations (PSYOPS) (Kallmeier et al. 2001). The CIMIC and PSYOPS operations now days constitute a significant portion of the total military effort. In effect, the forces engaged in operations not Art. 5/St.Petersburg, both for their value in the territory that for the external visibility of the operations themselves, are under the world opinion evaluation (Haugh 2000; Hue 2007; AJP-3.10.1; AJP-9).

CIMIC and PSYOPS are critical issues in S&R (Stabilization and Reconstruction) operations as well as during Stabilization and Normalization phases of most of current scenarios (Rehse 2004; Rietjens & Bollen 2008).

The authors present CAPRICORN Project that is devoted to the creation of new IA-CGF specific for the simulation of CIMIC and PSYOPS, able to consider key operational and territorial factors, and to the development of a demonstrator, able to show Modeling and Simulation potentials and capabilities in supporting Operational Planning (Bruzzone, Frydman & Tremori, 2009; Bruzzone et al. 2010). In effect Simulation represents one of the most important approaches to address this context even due to the high influence of stochastic factors and the complexity of the system, including social, economic, political, cultural and psychological aspects (Amico et al. 2000).

This paper proposes an overview of CAPRICORN Project concepts and Models and present the experimentation carried out to test and validate the proposed simulation model.

2. CAPRICORN PROJECT OVERVIEW

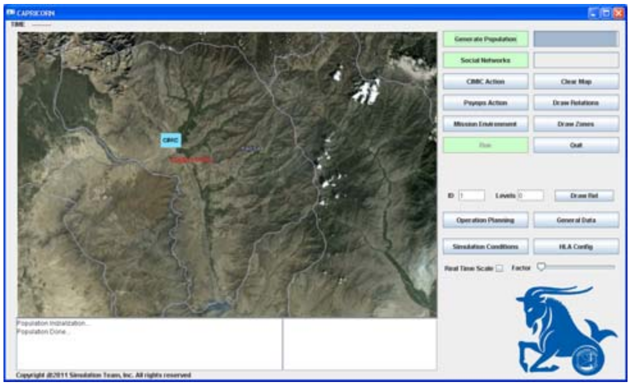
The research is related to CAPRICORN R&D Project (CIMIC and Planning Research In Complex Operational Realistic Network), that is an EDA (European Defense Agency) project sponsored by Italian and French Ministry of Defense and it is devoted to the development of capabilities in the complex and critical sector of Military Operation Planning, specifically for Not-Article5/San Petersburg Operations (Bruzzone, Frydman, Tremori 2009). CAPRICORN Project was lead by DIPTEM University of Genoa in partnership with LSIS, MAST srl and ITESOFT (acting as subcontractor of LSIS) and patronage from Liophant Simulation and Simulation Team.

The CAPRICORN Project main objectives are:

1. Define requirements and features to investigate Basic Operational Planning. One of the final goal is to provide simulation users with intelligent CGF (computer generated forces) and with the capability to elaborate and verify in normalization and stabilization scenarios operational plans foreseeing events where coalition forces, local population and non conventional Op-forces (e.g., terrorism, peace-keeping, peace-enforcing, urban riots, etc.) are involved .
2. Analyze the Human Behavioral Factors to be modeled in order to improve realism and reliability of the simulations results considering aspects related to both psychological and sociological aspects for representing collective behavior (problems: psychology, cultural, social, etc) (Bruzzone 2010).
3. Develop CIMIC, PSYOPS Humanitarian support or other non-conventional operations models by CGF managed by Intelligent Agents (Bruzzone & Massei 2010).
4. Enhanced Interoperable Multilevel Models: improve the PIOVRA project capability for the creation and management of interoperable multilevel models (Bruzzone et al. 2004).

The final goal of the project was to create a demonstrator using the up-to-date development in Interoperable Simulation in order to integrate all the different components in the CAPRICORN Demonstrator/Federation.

Simulators such as CAPRICORN guarantee a methodical simplification and an improved accuracy into the military operational planning processes; in effect the use of simulation in this context speeds up planning generation enabling the development of simpler and emendable plans in accordance with real life elements, scenario evolution and parameters changes (Bruzzone, Tremori & Massei 2011). Therefore in order to be effective in operational planning these simulators require to integrate advanced models and algorithms capable to reproduce complex scenarios as well as a robust and rational Validation and Verification process that should be applicable by users in short term and the limited resources (Bruzzone et al., 2009). CAPRICORN is focusing on identifying the requirements and developing models and algorithms for this application. The purpose is to provide a simulation system capacity to carry out an evaluation of effectiveness of various hypothetical courses of action. In addition CAPRICORN model is designed based on an HLA federation in order to integrate it with other models and tools and simulate in a more realistic and detailed way the effects that may have CIMIC activities (or PSYOPS).



Population Initialization...
Population Done...

Figure 1. CAPRICORN Demonstrator

3. CAPRICORN MODELS AND KEY ASPECTS

CAPRICORN Simulation Model is based on the concept of Multilevel Modeling. As matter of fact, CAPRICORN Objects are organized by a multilevel approach and some concepts are inspired by PIOVRA models (a previous EDA Project devoted to develop new Intelligent Agents to reproduce units such as Urban Rioters, gangs, police etc.), where the structure was based on Action Objects (entity on the field) and Comportment Objects (Organizations/Groups with specific attitudes). Anyway CAPRICORN context is more complex due to several aspects (Bruzzone & Massei 2007; Bruzzone, Massei et al. 2011) :

- Importance to identify, not only, the HBM and its evolution, but even to direct emotions and attitudes to specific subjects based on the events and actions as well as on the people perception (i.e. an attack to the population should be attributed to the insurgent or to the coalition by a village depending on its point of view and awareness)
- Necessity to model a small region, district or village group in order to support decisions related to activities with an impact on a large area
- Medium Long Time Simulation with more articulated effects of HBM (Human Behavior Modifiers) respect short time simulation
- Necessity to model the change of attitude and profile of the population along time simulation as result of CIMIC/PSYOPS activities

- Higher importance of Social and Cultural Background in addition to psychological factors (i.e. religion, ethnic group)

Due to these reasons the CAPRICORN models have a specific structure tailored for these cases; in particular the objects related to modeling the humans in CAPRICORN are represented in two major classes: People and Groups; People and Group classes are the basis to instantiate objects; each of this object will be driven by an intelligent agent in coherence with its characteristics, history and scenario awareness (Bocca et al. 2007; Bruzzone 2008).

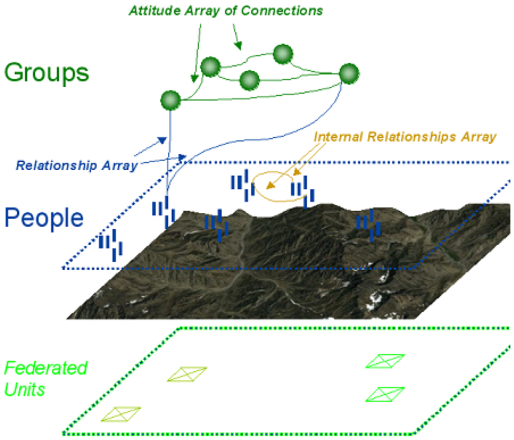


Figure 2. CAPRICORN Multilevel Model & Conceptual Architecture

The People Layer reproduces the individual and small group/entities. In addition in CAPRICORN there is a specific class for representing units on the field (i.e. a platoon taking care of patrolling activities, intelligence assets, logistics units, NGO), while CAPRICORN Action Object are devoted to reproduce Units and Special Entities operating on the field, in addition Activity Objects represent activity or task that could require People, Action or Group support and that are used to model the CIMIC and Psyops Courses of Actions.

A new challenging issue is related to Social Network Modeling in term of relationships generation and evolution (Bruzzone et al.2009). People Objects in CAPRICORN represent elements of the population and they have their own social network at their level; this network is defined by links (i.e. family, work position). Therefore in addition to these social networks the People Objects could be related even to higher level entities defined as Group Object (i.e. interest groups such as farmers or elders); however the dependence of People and Group objects could be structured on multilayers.

In fact Group Objects are even related among themselves; and each people object could be linked to several Group Objects as well as to several other people objects, in similar way group objects could be related each other.

In addition relations are even used to model all the links referring to People attitudes; these relations are not just discrete set of values (i.e. neutral, foe, friend), but results from the belonging to groups and to people/unit characteristics by the fuzzy variables; in fact these relations, as all the relations, are defined by using fuzzy representation.

In general the relations are defined in term of type, connected objects and attitude; the attitude is a fuzzy variable able to reproduce smooth and mixed feelings (i.e. friend 5%, indifferent 40%, hostile 55%); there are different kind of links that are classified as following:

- Attitude Connections: these links connect the group objects among themselves, these connections define how strong is the relation and how it is articulated (i.e. negative 30%, neutral 20%, positive 50%)
- External Relationships: this class of links connects a people object with a group object; each people object could be connected to multiple groups and in each relationship it is defined the strength characterizing the link as well as the attitude (i.e. positive or negative)
- Internal Relationships: this class of links connects people object among themselves

So considering the above mentioned list of relationships it is possible to define the structure of the social networks; for instance People Objects are characterized by a list of Internal Relationships that keep memory of family, work and friendship relations through links to other corresponding people objects. Group objects are also characterized by Lists of Attitude Connections. This approach allows to register actions impacts and effects on the single individual through their social network as well as on their group of interest. This means that if an action has a negative impact on a person belonging to a specific group, all the members of that group will be influenced, obviously with an impact that depends on several factors (i.e. attenuation factors, importance of the individual in the group, threshold levels for the perception, etc).

Obviously CAPRICORN Project introduced new intelligent agents specific for CIMIC and PSYOPs operations simulation and to model human behavior modifier, with special focus on trustiness among two people or groups.

In addition for the Population generation, the Group Configuration Objects are introduced in order to generate statistical distributions based on historical data and hypotheses to define people characteristics. These objects identify the different groups in term of social, religious, political, ethnic and physiological aspects. The Population is created for each statistical group in references with their statistical characteristics based on Monte Carlo Technique extracting data from defined statistical distributions based on Group Configuration Objects. Therefore in CAPRICORN the population is driven by agents and the virtual people are generated by applying Monte Carlo Technique to specific group statistics in order to represent a region. Each agent is assigned to places inside different zones in term of Home and Working location based on compatibility algorithm.

4. CAPRICORN DEMONSTRATOR

CAPRICORN Demonstrator is developed on Windows environment and implemented by using Java language. The CAPRICORN Demonstrator Development is based on the strong involvement of military users for: requirements collection, design, implementation, validation and verification, maintenance (Bocca et al. 2010; Bruzzone & Massei 2011). So, all the results are compared and evaluated with users expectations and requirements. Therefore during the software development, user feedback was very critical during the whole process.
The CAPRICORN Demonstrator includes a Mission Environment Generator and a Simulator; the internal architecture of the Simulator is based on stochastic discrete event simulation and applies Scan and Rescan scheme on the event.

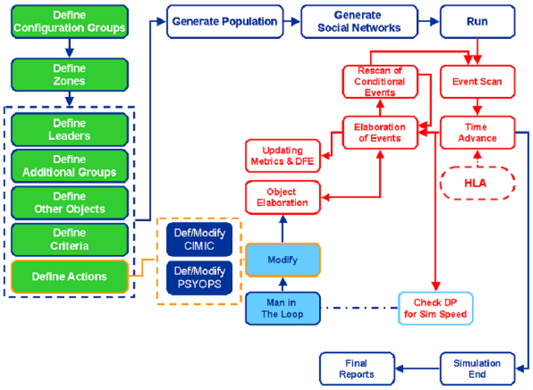


Figure 3. CAPRICORN Acquisition & Simulation architecture within CAPRICORN Demonstrator

The CAPRICORN Demonstrator generates the population and social networks based on Monte Carlo Technique; the people and groups generated interact with the action objects and CIMIC/PSYOPS applying discrete-event methodology; the parameters related to actions and events are regulated by stochastic phenomena (i.e. setting time to be ready to move); dynamically during each simulation and starting from random seed related to the specific experiment, the CAPRICORN Simulation extract by Monte Carlo Technique, the required values from statistical distributions used to reproduce the stochastic factors
The following active functions are provided to the users:
- Mission Environment Definition: before running the simulation, the user is required to set up the Mission Environment by defining all the boundary conditions for a Specific Scenario (i.e. Configuration Groups, Zones & Areas, Leaders, Additional Groups).
- Operational Planning: the user is able to add new actions (CIMIC/PSYOPs) or modify the existing ones before the simulation execution or during the run execution.
- Definition of Simulation Parameters and Run: the user is allowed to set the simulation conditions (such as simulation duration, time factor, HLA mode); to generate the population and the social networks and to run the simulation.

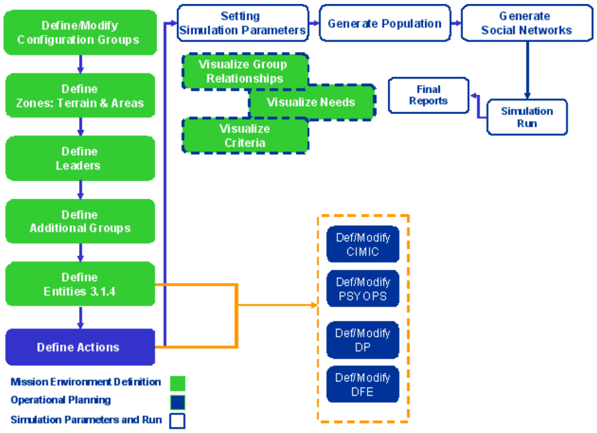
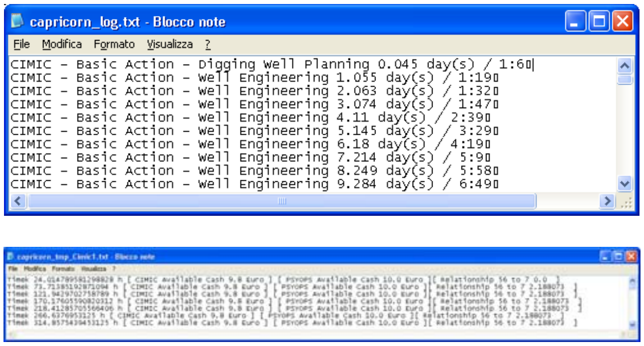


Figure 4. CAPRICORN Demonstrator functions

The CAPRICORN Simulation allows to investigate how a mission plan (CIMIC or PSYOP) affects human behaviour and social network, in particular it provides different outputs related to:

- Information about the action process (phases, time, costs and involved resources)
- Information about the relationship evolution between the groups involved in the action

So the final outputs present the following information:
-CIMIC Phase and correspondent time
- Time, available Cash for CIMIC, available Cash for PSYOP, Relationship ID e Trustiness Level
For instance for a Digging Well operation the reports are like the following:


capricorn_log.txt - Blocco note
File Modifica Formato Visualizza ?

```
CIMIC - Basic Action - Digging Well Planning 0.045 day(s) / 1:6▯
CIMIC - Basic Action - Well Engineering 1.055 day(s) / 1:19▯
CIMIC - Basic Action - Well Engineering 2.063 day(s) / 1:32▯
CIMIC - Basic Action - Well Engineering 3.074 day(s) / 1:47▯
CIMIC - Basic Action - Well Engineering 4.11 day(s) / 2:39▯
CIMIC - Basic Action - Well Engineering 5.145 day(s) / 3:29▯
CIMIC - Basic Action - Well Engineering 6.18 day(s) / 4:19▯
CIMIC - Basic Action - Well Engineering 7.214 day(s) / 5:9▯
CIMIC - Basic Action - Well Engineering 8.249 day(s) / 5:58▯
CIMIC - Basic Action - Well Engineering 9.284 day(s) / 6:49▯
```

capricorn_tmp_Cimic1.txt - Blocco note
File Modifica Formato Visualizza ?

```
Time: 24.014789581298828 h [ CIMIC Available Cash 9.8 Euro ] [ PSYOPS Available Cash 10.0 Euro ][ Relationship 56 to 7 0.0 ]
Time: 73.71385192871094 h [ CIMIC Available Cash 9.8 Euro ] [ PSYOPS Available Cash 10.0 Euro ][ Relationship 56 to 7 2.188073 ]
Time: 121.9429702758789 h [ CIMIC Available Cash 9.8 Euro ] [ PSYOPS Available Cash 10.0 Euro ][ Relationship 56 to 7 2.188073 ]
Time: 170.17605590820312 h [ CIMIC Available Cash 9.8 Euro ] [ PSYOPS Available Cash 10.0 Euro ][ Relationship 56 to 7 2.188073 ]
Time: 218.41285705566406 h [ CIMIC Available Cash 9.8 Euro ] [ PSYOPS Available Cash 10.0 Euro ][ Relationship 56 to 7 2.188073 ]
Time: 266.6376953125 h [ CIMIC Available Cash 9.8 Euro ] [ PSYOPS Available Cash 10.0 Euro ][ Relationship 56 to 7 2.188073 ]
Time: 314.8575439453125 h [ CIMIC Available Cash 9.8 Euro ] [ PSYOPS Available Cash 10.0 Euro ][ Relationship 56 to 7 2.188073 ]
```

Figure 5. CAPRICORN Report

Obviously it is possible to plan a set of CIMIC and PSYOPs actions in different zones and affecting different groups; so it will be available the overall report including the information related to their development and their impact on the population. CAPRICORN Simulation results are therefore useful to evaluate and test different mission plans in order to take in account the possible effects of these actions on the population behavior.

5. CAPRICORN EXPERIMENTATION

The Experimentation Plan is included in the VV&A (Verification, Validation and Accreditation) Process and it includes two main phases, one devoted to review requirements and involve Subject Matter Experts and military users in order to obtain feedback and comments about CAPRICORN conceptual Models and CAPRICORN Demonstrator Specifications; the second devoted to define together with selected users (CAPRICORN Users Champion) a Specific Mission Environment to be simulated and run (Tremori et al. 2009; Frydman et al. 2011). In particular CAPPRICORN Demonstrator is set in Kapisa, the smallest Afghan Region and it allow to simulate the following CIMIC and PSYOPs operations (Digging Well, Building Police Station, Building a School, Radio Messages, TV Shows, Leaflet). Therefore CAPRICORN Experimentation has strongly involved military users and subject matter experts to:

- collect users requirements
- develop and validate CAPRICORN conceptual models
- define the specific mission environment implemented in CAPRICORN Demonstrator
- validate the Demonstrator functions and features including interoperability capability
- test CAPRICORN Demonstrator and analyze simulation results

Along the whole project several meetings and workshops were held with Subject Matter Experts and Users Champion and CAPRICORN Experimentation is set up to allow users to test directly the demonstrator both in stand alone and federated mode. In particular these events were carried out:

- Preliminary National Testing & Experimentation to finalize details and solve bugs, problems and misunderstanding; this activity is carried out in cooperation by CAPRICORN Partners and CAPRICORN Champions
- Final National Experimentation to demonstrate the CAPRICORN Demonstrator Capabilities and proposed approach; this activity is carried out in cooperation by CAPRICORN Partners and CAPRICORN Champions
- Synthetic Experimentation Presentation to exploit the CAPRICORN Project Result in National MoD Communities; this activity is carried out in cooperation by CAPRICORN Partners and CAPRICORN Champions

6. CAPRICORN EXPERIMENTAL ANALYSIS

The authors provide the experimental analysis carried out through the final reports of CAPRICORN simulation; in effect it is possible to evaluate and test different courses of actions by planning and simulating different CIMIC/PSYOPs in term of type, location, target group, promoting group, duration, budget, resources.

Concerning with the experimental analysis, the authors applied Mean Square pure Error and Sensitivity Analysis for different CIMIC & PSYOP actions by considering a 2-level factorial design respect to the trustiness level as target function.

For instance, considering a CIMIC action Digging Well from COA pro Sunni in Zone 0 the MSpE (Mean Square pure Error) was the following:

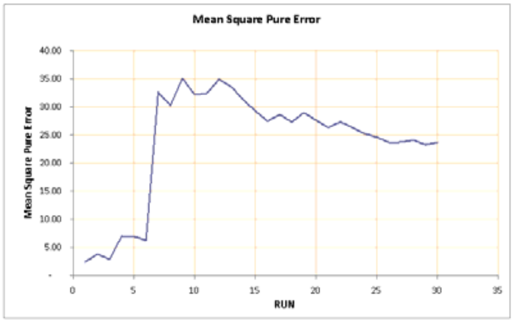
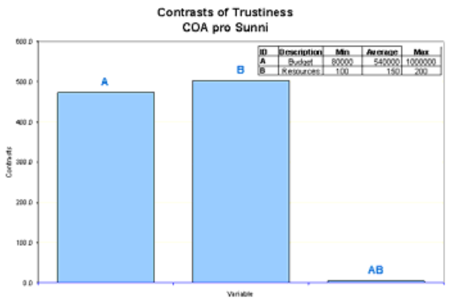


Figure 6. Mean Square pure Error Diagram for a CIMIC action Digging Well from COA pro Sunni in Zone 0 (Run expresses the pure number of replications; MspE express the trustiness variance; Trustiness [-100 to 100])

The Experimental Error is stable between the 26th to the 30th run. So it is possible to state that 26 run are needed for a correct evaluation of the experimental error.

By considering the sensitivity analysis related to the independent variables Resources and Budget, both are significant and have positive effects on the population trustiness level:



ID	Description	Min	Average	Max
A	Budget	80000	540000	1000000
B	Resources	100	150	200

Figure 7. Contrasts Diagram related to Trustiness Target Function respect of Budget and Resources (Contrast represent the influence of a factor expressed respect trustiness as scalar [-100 to 100]; Budget [Euro] and Resource [people])

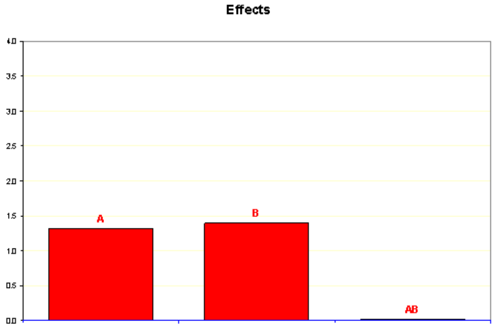


Figure 8. Effects Diagram related to Trustiness Target Function respect of Budget and Resources (Effect represent the influence expressed as ratio between contrast2 and the square pure error of trustiness scalar [-100 to 100]; A is the Budget; B the Resources and AB their combined effect)

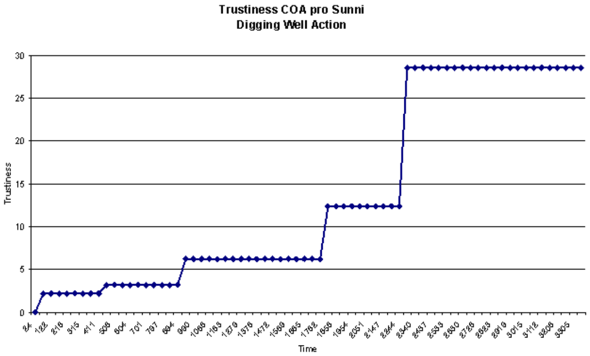


Figure 9. Trustiness evolution during the simulation of a CIMIC action Digging Well from COA pro Sunni in Zone 0 (Trustiness is expressed as scalar [-100 to 100]; Time [h])

Other experiments were carried out by considering different CIMIC and PSYOP actions.

In the following table it is proposed a comparative analysis carried out by ranking solutions in term of trustiness improvement [pure number]

Ranking	*COA*	*Budget*	*Resources*	*Who*		*Where*	*What*	*Trustiness Improvement*
1	**CIMIC1**	**1'000'000**	**200**	**Coa?**	**Sunni**	**Zone 0**	**Digging Well**	**43.79994**
2	PSYOPS1	500'000	200	Coa?	Sunni	Kapisa	Radio messages	43.182137
3	CIMIC1	80'000	200	Coa?	Sunni	Zone 0	Digging Well	26.775768
4	CIMIC1	1'000'000	100	Coa?	Sunni	Zone 0	Digging Well	26.299814
5	PSYOPS1	100'000	200	Coa?	Sunni	Kapisa	Radio messages	19.60504
6	PSYOPS2	150'000	150	Coa?	Sunni	Kapisa	TV messages	15.526324
7	PSYOPS2	50'000	150	Coa?	Sunni	Kapisa	TV messages	13.418227
8	CIMIC1	80'000	100	Coa?	Sunni	Zone 0	Digging Well	12.568763
9	PSYOPS1	500'000	100	Coa?	Sunni	Kapisa	Radio messages	7.4699154
10	PSYOPS1	100'000	100	Coa?	Sunni	Kapisa	Radio messages	4.743664
11	PSYOPS2	150'000	50	Coa?	Sunni	Kapisa	TV messages	4.72036
12	PSYOPS2	50'000	50	Coa?	Sunni	Kapisa	TV messages	4.118518
13	CIMIC2	150'000	150	Coa?	Shia	Zone 4	School Building	1.81875207
14	CIMIC2	50'000	150	Coa?	Shia	Zone 4	School Building	0.74382114
15	CIMIC2	150'000	50	Coa?	Shia	Zone 4	School Building	0.64544094
16	CIMIC2	50'000	50	Coa?	Shia	Zone 4	School Building	0.43958664

Figure 10. Comparative Analysis among Different Course of Actions

In the following figure it is proposed the comparison in term of result distribution between two alternative CIMIC COA (two different budgets); this risk analysis allows to identify the distribution of the results in statistical terms

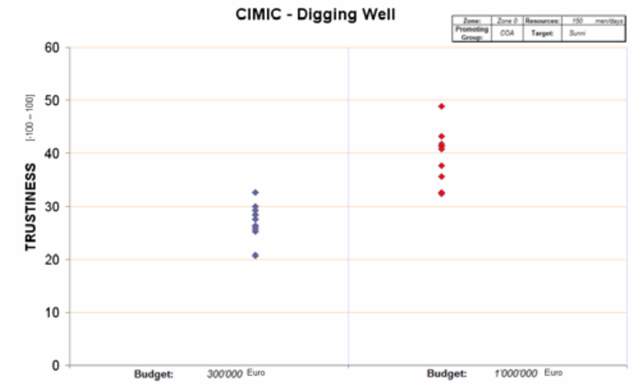


Figure 11. Comparison between two alternative CIMIC COA

7. CONCLUSIONS

The research addresses the problem of providing support in evaluating complex situations dealing with human factors in order to complete scenario analysis or decision making; the context of application is related to operational planning with special attention to stabilization and normalization process and to CIMIC and PSYOPS operations. The authors propose a simulation model, called CAPRICORN, to demonstrate the potential of the M&S use as a virtual framework to investigate alternative hypotheses on the scenario and different decision impacts. This simulator is designed for being used both by operational planners and trainers. Obviously, considering the high influence of HBM (Human Behaviour Modifiers), the resulting simulation solutions are not expected to be predictive tools, vice versa their goal is to estimate risks and confidence bands related to different alternatives.

The authors propose the CAPRICORN Experimentation carried out with military users and some experiments in order to test different alternative actions to evaluate the CIMIC and PSYOPs operations impacts and effects on local population in term of trustiness level.

The proposed experimentation is part of the CAPRICORN VV&A process and it shows the capability to quickly acquire data and analyze different hypotheses by using intelligence report estimation and operational people estimations.

AKNOWLEDGEMENT

The authors are very glad to thank the EDA and the Italian and French MoD (Minister of Defense) that are sponsoring CAPRICORN Project. For further information please visit www.liophant.org/projects/capricorn.

REFERENCES

AJP-3.10.1, "NATO psychological operations doctrine", NATO/PfP unclassified

AJP-9, NATO civil-military co-operation (CIMIC) doctrine, NATO/EAPC unclassified

Amico Vince, Guha R., Bruzzone A.G. (2000) "Critical Issues in Simulation", Proceedings of SCSC, Vancouver, July

Bocca E., Pierfederici, B.E. (2007) “Intelligent agents for moving and operating Computer Generated Forces”, Proc.of SCSC, San Diego July

Bocca E., Massei M. et al. (2010) "Italian Requirements on Simulation and CGF for Operation Planning", Simulation Team Technical Report, Genoa

Bruzzone A.G., Massei M. (2011) "Objective System Specification for CAPRICORN Project", Simulation Team Technical Report, Genoa

Bruzzone A.G., Massei M. et al. (2011) "Review of Methodologies and technologies used in PIOVRA to be reused and/or adapted for CAPRICORN", Simulation Team Technical Report, Genoa

Bruzzone A.G. Tremori A., Massei M. (2011) "Adding Smart to the Mix", Modeling Simulation & Training: The International Defense Training Journal, 3, 25-27, 2011

Bruzzone A., (2010) “Human Behaviour Modelling as a Challenge for Future Simulation R&D: Methodologies and Case Studies”, Plenary Speech at Eurosim 2010, Prague

Bruzzone A.G., Massei M. (2010) "Intelligent Agents for Modelling Country Reconstruction Operation", Proceedings of AfricaMS 2010, Gaborone, Botswana, September 6-8

Bruzzone A., Madeo F., Tarone F., (2010) “Modelling Country Reconstruction based on Civil Military Cooperation”, Proc. of I3M2010, Fez, Oct.

Bruzzone A.G., Massei M., Tremori A., Bocca E., Madeo F. (2010) "Advanced Models for Simulation of CIMIC Operations: Opportunities & Critical Issues Provided by IA", DIFESA2010, Rome, Italy

Bruzzone A.G., Reverberi A., Cianci R., Bocca E., Fumagalli M.S, Ambra R. (2009) "Modeling Human Modifier Diffusion in Social Networks", Proceedings of I/ITSEC2009, Orlando, Nov-Dec

Bruzzone A.G., Frydman C., Cantice G., Massei M., Poggi S., Turi M. (2009) "Development of Advanced Models for CIMIC for Supporting Operational Planners", Proc. of I/ITSEC2009, Orlando, November 30-December 4

Bruzzone A.G., Frydman C., Tremori A. (2009) "CAPRICORN: CIMIC And Planning Research In Complex Operational Realistic Network" MISS DIPTEM Technical Report, Genoa

Bruzzone A.G. (2008) "Intelligent Agents for Computer Generated Forces", Invited Speech at Gesi User Workshop, Wien, Italy, October 16-17

Bruzzone A.G., Scavotti A., Massei M., Tremori A. (2008) "Metamodelling for Analyzing Scenarios of Urban Crisis and Area Stabilization by Applying Intelligent Agents", Proceedings of EMSS2008, September 17-19, Campora San Giovanni (CS),Italy

Bruzzone A.G., Massei M. (2007) "Polyfunctional Intelligent Operational Virtual Reality Agent: PIOVRA Final Report", EDA Technical Report

Bruzzone A. G et al. (2004) "Poly-Functional Intelligent Agents For Computer Generated Forces", Proceedings of the 2004 Winter Simulation Conference Washington D.C., December

Caussanel J., Frydman C., Giambiasi N., Mosca R. (2007) “State of art and future trend on CGF” Proceedings of EUROSIW2007, Santa Margherita, Italy, June

Chauvancy F. (2011) “Réflexions militaires sur les opérations d’influence dans le cadre de la stabilization”, Séminaire « Compréhension des paramètres d’environnement dans les opérations de stabilisation », Université des Sciences de Marseille, 5 janvier 2011

Fletcher M., (2006) “A Cognitive Agent-based Approach to Varying Behaviours in Computer Generated Forces Systems to Model Scenarios like Coalitions”, Proceedings of the IEEE Workshop on Distributed Intelligent Systems: Collective Intelligence and its Applications,

Frydman C., Massei M. et al. (2011) "Definition of Metrics and Validation, Verification and Plans", Simulation Team Technical Report, Marseille

Galula D., (1964) “Counterinsurgency Warfare”, Praeger Security International

Haugh, B. and Lichtblau, D., (2001) “An Information Technology Support Strategy for PSYOP Impact Analysis,” IDA Paper P-3587, Institute for Defense Analyses, February

Haugh, B. and Lichtblau, D., (2000) “PSYOP Impact Analysis White Paper,” IDA Paper P-3060, Institute for Defense Analyses, August

Hue B., EMA/CPCO2J9, (2007) “What Do CIMIC Activities Bring to Stabilization1 Operations”, France, Doctrine General Military Review #12, page 29

Kallmeier V., Henderson S., McGuinness B., Tuson P., Harper R., Price S. Storr J. (2001) "Towards Better Knowledge: A Fusion of Information, Technology, and Human Aspects of Command and Control", Journal of Battlefield Technology, Volume 4 Number 1.

Lichtblau, D., et al., (2004) “Influencing Ontology,” extended abstract in Behavior Representation in Modeling and Simulation Conference

Rietjens S.J.H., M. Bollen, (2008) “Managing Civil-Military Cooperation”, Military Strategy and Operational Art

Nacer A., Taylor A., Parkinson G. (2007) “Comparative Analysis of Computer Generated Forces” Artificial Intelligence, Ottawa

Rehse P., (2004) “CIMIC : Concepts, Definitions and Practice”, Heft 136, Hamburg, June

Thagard, P., (2000) Coherence in Thought and Action, Cambridge, MA: MIT Press

Tremori A., Bocca E., Tarone F., Longo F., Poggi S. (2009)"Early Testing Procedures For Supporting Validation Of Intelligent Agents For Simulating Human Behavior In Urban Riots", Proceedings of MAS2009, Tenerife, September

Authors' Index