MODELING CYBER WARFARE IN HETEROGENEOUS NETWORKS FOR PROTECTION OF INFRASTRUCTURES AND OPERATIONS

Agostino G. Bruzzone, Diego Merani
NATO STO CMRE
Email: {bruzzone, merani}@cmre.nato.int
URL: www.cmre.nato.int

Marina Massei, Alberto Tremori
DIME University of Genoa, Italy
Email: {massei, tremor}@itim.unige.it
URL: www.itim.unige.it

Christian Bartolucci, Angelo Ferrando
Simulation Team
Email: {Christian.bartolucci, angelo.ferrando}@simulationteam.com
URL: www.simulationteam.com

ABSTRACT
This paper presents a modeling approach for mapping cyber defense issues with respect to heterogeneous networks; the research is devoted to develop an agent driven simulation environment able to analyze this problem considering different layers including CIS capabilities, operational issues, system architecture, management processes and human factors. The paper analyzes a specific case study to validate and verify the proposed modeling approach; the scenario is focused on an heterogeneous network applied to extended maritime environment including Autonomous Underwater Vehicles (AUV), sensors, platforms, vessels, satellites and relevant military assets and threats. The present document uses this case study as example of System of Systems to be simulated including cyber warfare issues to evaluate their impact on operations.

keywords: Cyber Defense, Interoperable Simulation, Maritime Simulation, Heterogeneous Networks, Autonomous Systems, Modeling & Simulation

1. INTRODUCTION

The research aims at matching the NATO Topology of Heterogeneous Networks with Cyber Defense warfare in order to model the different elements and possible risks (i.e. installation procedures, access methods, training level, networking reliability, data certification, encryption procedures, password management, operator procedure etc.).
Heterogeneous Networks are becoming popular and intensively present in several application areas, since they represent an opportunity and have a big potential, while at the same time introduce new open issues and problems: indeed these systems, whose capability is affected by multiple layers, involve complex phenomena such as data abundance that overpasses the elaboration capabilities, hiding techniques, non-collaborative targets behaviors, environmental conditions, assets reliability, models maturity, agility, node compromised resources, etc. Such increasing popularity is expected to become very common in military field as a consequence of the technology evolution trends with special attention to autonomous systems, robots and sensor networks (Bruzzone et al. 2005; Tether 2009). A great challenge for the near future is related to the possibility to link together lots of light mobile devices in order to have a complete persistent understanding of the battlefield and so get advantages in terms of military results, properly addressing cyber defense issues.
Due to the high level of interactions among the networks and their complexity, this application field requires to be investigated using M&S (Modeling and Simulation); indeed the presence of several stochastic factors affecting the behaviors of the different actors in the scenario needs to be modeled through

Intelligent Agents and properly mapping policies, doctrines as well as new potential threat behaviors.

2. INTEROPERABLE SIMULATION FOR CYBER WARFARE IN HETEROGENOUS NETWORKS

From this point of view, simulation is very important in reproducing heterogeneous networks considering the complexity of the different systems and interactions; in fact, following this approach, it becomes possible to model different devices linked together into a scenario, and to simulate the different layers covering technological, operational and social aspects.

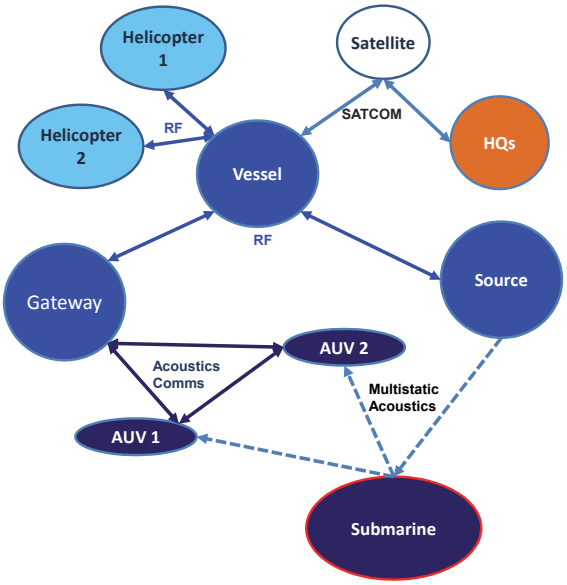

Figure 1: Example of heterogeneous network for an ASW operation involving 2 AUVs

Vice-versa, it could be very difficult to test the effectiveness of this System of Systems in the real context and to identify architectures and actions able to improve it with a convenient cost/benefit rate considering the complexity of the framework, the high concentration of parameters and the number of entities involved. In addition simulation allows users to insert into the scenario new concepts and technologies and to analyze the network performance with respect to introduced threats and considering the interactions among systems and components; by this approach it becomes possible to evaluate in a virtual simulation environment the system capabilities and to finalize new requirements and/or procedures (Hua Guo et al. 2010).

In this context, one of the main goals of this research is to couple topologies and characteristics of heterogeneous networks and cyber defense warfare within conceptual models ready to be federated and simulated; this research aims at defining models reproducing objects, attributes and their behaviors and interactions to reproduce heterogeneous networks immersed in operational scenarios and operated by human social networks.

The authors are currently working on researches related to Marine heterogeneous Network involving autonomous vehicles, satellites, vessels, aircrafts, sensors and emitters as proposed in figure 1 (Bruzzone et al 2013; Wiedemann 2013); these heterogeneous systems could be devoted to conduct different complex missions such as Intelligence, Surveillance and Reconnaissance (ISR). Indeed, these heterogeneous networks result as an aggregation of different assets (i.e. underwater systems, surface drones, ships, helicopters and even satellites) being available for connection on based on their operative status and boundary conditions; this context is a very sensitive environment to cyber warfare issue; in this area the conceptual models are representing the characteristics of nodes, connections, infrastructures of the heterogeneous network; the different models could be implemented in different simulations able to be federated together over the operational scenario by using HLA (Bruzzone et al. 1998; Kuhl et al. 1999; Massei et al. 2013); in addition to these models, even the procedures related to the social layer could be simulated within stochastic discrete event models and synchronized in this federation (Massei and Tremori 2010). These simulated layers federated together represent the environment available to conduct tests and experimentations for high fidelity simulation as well as for preliminary investigations. The authors are currently focusing their attention on the maritime extended framework including multiple domain such as sea surface, underwater, air, space, cyberspace, land and coast (Bruzzone 2013); in this context security issues as well as cyber warfare are critical elements (Longo et al. 2005; Bruzzone, Massei, Tremori, Longo, Madeo, Tarone 2011)

3. CONTEXT OVERVIEW

Cyber security is a major issue in the industrial and business sectors, especially in relationship with emerging contexts such as power grid (Yang et al. 2011) and SCADA systems (Urias et al., 2012). A methodology for analyzing the compromise of a deployed tactical network has been proposed by Asman, B.C. et al. in 2011. Homeland security applications were approached in 2007 by Kotenko, I. in its work on Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense; a recent work on how to mitigate a cyber-physical attack that

disables the transportation network and releases a cloud of chlorine gas has been published by the U.S. Dept. of Homeland Security, whose security analysts developed simulation models and tools to analyze the consequences of complex events on critical U.S. infrastructure and resources (Nabil Adam et al., Communications of the ACM, no.56/6, June 2013); the analysis of ICT infrastructures respect cyber security issues could be addressed even by risk analysis and Monte Carlo Simulation using HPC (High Performance Computing) to solve the computational workload (Baiardi et al, 2011); therefore in most of the cases it could be necessary to include the stochastic components with functional and operational models; for instance this paper addresses the point of combining actions over the real with the cyber battlefield in a coordinated way, indeed this point is supposed to have a major impact on future war operations (Jakobson 2004).

These problems strongly affect the nature of heterogeneous networks that is characterized by dynamic and complex nature (Rumekasten 1994). The use of intelligent agents has been demonstrated very effective for reproducing reactive entities and complex systems; the concept of agent driven simulation where the IAs (Intelligent Agents) are directing objects active within the simulation were experimented in a wide spectrum of applications (Oren and Ylmaz 2009). Indeed the capability to reproduce by agent emergent behaviors in complex system is major benefit of this approach (Thompson and Bossomaier 2006).

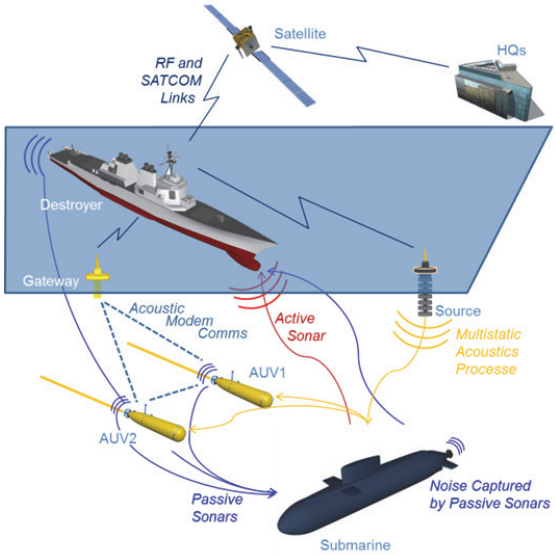

Figure 2: Sensor Network Case Study

The IA allows modeling platforms, humans as well as their interactions (Cornforth et al. 2004; Calfee and Rowe 2004).

The authors have long experience in using intelligent agents for reproducing intelligent reactive behaviors within complex mission environments (Bruzzone 2008; Bruzzone 2010); obviously the intelligent agents could implement different AI (Artificial Intelligence) techniques and methodologies (Bruzzone, Massei, Tarone, Madeo 2011; Affenzeller et al. 2009). Indeed the proposed scenario where AUV operates requires also coordination among Autonomous system that could be directed by the humans just when communication are working over the network; the problem of coordination among UAS (unmanned autonomous systems) has been investigated in order to identify proper approaches and effective control solution (Feddema et al. 2002; Vail and Veloso 2003; Kalra et al. 2010); indeed this problem represents a very good case of heterogeneous network where it is possible to apply different methodologies (Tanner 2007); the problem was even addressed with specific reference to marine mission environments (Merkuriev Y. et al. 1998; Sujit 2009; Martins et al. 2010; Nad et al. 2011; Zini 2012).

4. MODELS & SCENARIO

This research, through its topological approach over heterogeneous networks, is devoted to create a Federation of models based on HLA simulation interoperability standards (i.e. High Level Architecture); such federation should be able to couple the different models and layers related to such kind of networks and to simulate their interactions with respect to operational scenarios. In particular it focuses on cyber defense topological and procedural aspects regarding complex heterogeneous networks; one crucial part it is represented by introducing autonomous and intelligent behavior over the simulated entities, in this case the simulator was adopting Intelligent Agents Computer Generated Forces (IA-CGF) developed by Simulation Team to reproduce threats, behaviors as well as entities reactions (Bruzzone, Tremori, Massei 2011). The specific scenario used as test-case for this research is a surveillance system composed of unattended autonomous underwater sensors (AUV) whose mission is to detect an enemy target through sensing and collaboration via acoustic underwater communication. This system is able to perform different missions (e.g. area clearance or hold-at-risk in specific choke points).

The sensors communicate with a surface node (sink) which acts as a gateway between underwater and

above water communications systems. The surface node has the capability to connect with a local naval unit via Line of Sight RF link. The naval unit then provides data fusion and system integration with existing global C2 tactical networks via satellite communication capability (SATCOM) as proposed in figure 2.
The capability of Heterogeneous Networks are combined by the effect of different layers: a CIS layer including user applications, information system equipment, communications equipment, and user applications; but also an operational layer, including business processes (Information Assurance processes, Service Management and Governance processes etc.), information products and other operational capabilities directly connected or derived from the operation or mission type.

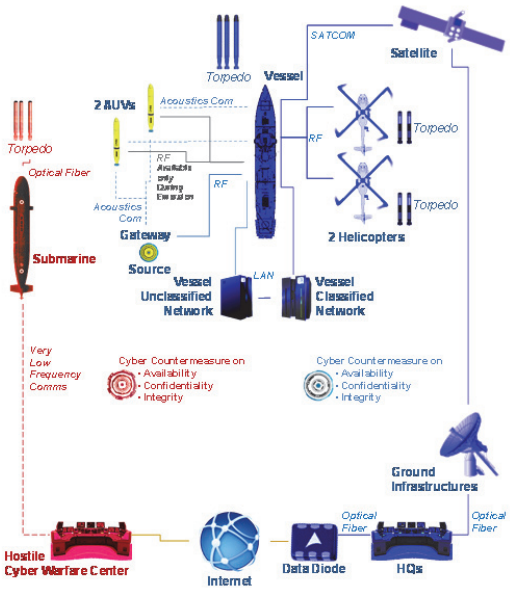

Figure 3: MCWS Objects

The model considers the distinction between the CIS infrastructure (Computer Information Systems representing the Cyber Infrastructure) and the operational context including the mission and operation type, and all user-related processes that form the operational capability.
Some human behaviors, in fact, could easily compromise a network or its performance due to accidental and/or intentional actions; as regards intentional ones, in some cases terrorists exploit procedural lacks in order to drive their attacks to success. It is interesting to note that even completely automated persistent solutions could quickly degrade their performance due to actions on the human layer. For this reason the Information Assurance components that influence the Operational Context (i.e. information products and the user-related processes) are included in the simulation in order to estimate their impact with respect to the other layers.
In addition to these elements, in defense scenarios key performance indexes and measures of merits are evaluated on the operational layer that is reproduced within the simulation environment: indeed the performance of the heterogeneous network should be tested with respect to the dynamic evolution of the operations since this affects the different alternative Course of Actions (COA).
A first step in the problem analysis is represented by the definition of node security properties through scoring of security properties such as Confidentiality, Integrity, Availability, Non-Repudiation and Authentication. Then criteria for modeling nodes performance in normal conditions, as well as their interaction with other nodes, are defined.
A third step is the simulation of the impact that a total or partial break-down of a node, consequence of a successful exploit of a vulnerability, would have on other network nodes, and on the overall performance of the system: such effects are evaluated in percentage points, but even in terms of operational impact (measured in the simulated environment). The choice to restrict the simulation to the vulnerability/threat pairs that determine the most relevant effects in terms of security capability over each node, along the simulation evolution, as well as to the resolution and the most significant details required to reproduce the different layers, is related to the possibility to finalize a relevant demonstration within the research timeframe; such finalization is made possible by the use of simplified meta-models able to approximate the behavior of the objects. Nevertheless the simulation architecture proposed guarantees the possibility to keep the proposed modeling approach open for further developments and even to replace some models in the future by more detailed ones (Zacharewicz et al. 2008).
In general the research includes among different layers the network models as well as cyber architecture objects. The simulated scenario is composed by sensors, entities that collect information from them, units on the field and a Command and Control Network. Not only networks nodes, but also links between them are often physical objects with specific properties (e.g. the LAN, Local Area Network, that connects two computers); the preliminary model was finalized in MCWS (Marine Cyber Warfare Simulator) developed in cooperation among the authors; this simulator does not include any sensitive information even if realistic data were used for the setup; in figure 3 it is proposed the set of

the objects representing the assets and connections simulated in the current scenario within MCWS, while its implementation in Java is proposed in figure 4; the HQs in fact is connected to the web adopting proper solutions for guaranteeing the protection of its own infrastructure (Bruzzone et al. 1999)

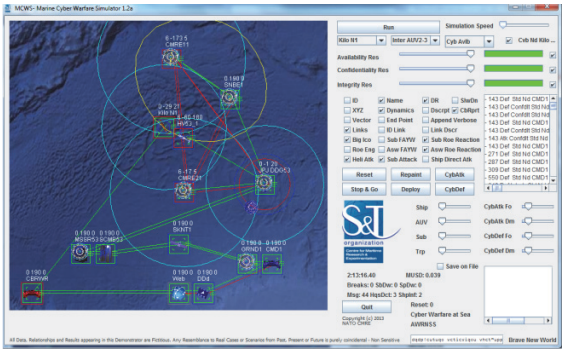

Figure 4: MCWS Simulator

The characterization of the security properties of the nodes, and the links between them, has been conducted through a process of identification of key properties and behaviors; for example, we assume that the Integrity factor of one network node affects downstream flows of information; or that the confidentiality of a node can be only compromised in its wholeness.
Nevertheless, the simulator can be fed with as many granular security properties or behavior as required, to augment its accuracy. The simulator is able to discriminate cases in which there is a monitoring activity over the nodes with respect to the cases in which such activity is not carried out, and to consider remediation actions in case a cyber-attack is detected.
After defining cyberspace objects with their variables, their attributes and their mutual interactions, input actions such as degrees of freedom as well as threats effects to be are identified: this is the scheme basing on which the model applies stochastic factors and probabilistic rules that reproduce how the exploitation of a node vulnerability influences the others. In a similar way, the operational layer, including user processes, is modeled and simulated even considering stochastic factors affecting the procedure evolution.
Behaviors and Rules of Engagements (ROEs) were implemented by configuring IA-CGF for the specific roles including: cyber warfare actions and operational decisions.

5. MCWS ANALYSIS AND EXPERIMENTATION

The scenario used to validate and verify MCWS was inspired by the case above described with some characteristics.
In the proposed scenario the Blue Force has the role to protect the area from submarines arriving from East; while the submarine (OPFOR) goal is move from West side up to the East borders over a square (20 by 20 nautical miles) in deep waters; however the operations are not limited to the square and could be extended even over it if necessary both by the submarine and the Blue Force. The environmental simulation includes sea current, wind, sea waves, weather conditions, temperature and visibility over day and night. Very simplified public release models have been adopted for sonar detection including:

- Passive Sonar the model are affected by target and sonar platform noise affected by dynamic behaviors as well as by the specific characteristics of the sensor
- Active Sonar Mono-static and Multi-static the model are affected by acoustic target strength and characteristics of the boundary conditions of the assets and sensors dynamically evolving during the simulation.

Blue Force resources include 2 AUVs, 1 Destroyer with 2 helicopters, 1 Buoy able to act as Emitter and gateway, a Satellite Network, a Ground Infrastructure and an HQs with web connection through a data diode; the helicopters and the ship are equipped with ASW (Anti-Submarine Warfare) torpedo and Vessel LAN is simulated as divided between classified Network connecting with HQs and unclassified network connecting AUV.
In this scenario, the Blue Force is not entitled to carry out offensive cyber-attacks, but could adopt preventive and reactive measures to protect their cyber space both in term of nodes and connections.
OPFOR have just a submarine armed with torpedo and a cyber-warfare center transmitting sensitive information through very low communication; in order to simplify the scenario the submarine cyber warfare center communication is consider very reliable over a wide spectrum of operational modes; obviously the reliability and availability of this connection could be consider subjected to all boundary and conditional factors as other connection in the future for more realistic researches.
In this scenario the focus is on the three among the node security properties:

- Availability: this element affects the reliability and throughput of network connections and nodes; if availability is completely disrupted the corresponding resources are not available at all; in this case rerouting is possible, if alternative paths exist.
- Confidentiality: this element measures the capability of Opposing Force (OPFOR) to access data and information present or passing through a network node or link; if this property is compromised and a message including position of an asset (i.e. an AUV or the Destroyer) pass through this cyber resource, the information is transmitted to the submarine who changes its behavior in order to respect the ROE (i.e. avoid contact).
- Integrity: this element measures the accuracy of the content of data (information); if integrity is compromised, the messages going through the compromised entity are disrupted or modified with unuseful or fake information, and cannot be processed; this affects obviously the command chain, therefore the message could be delivered over different paths where they are available, to solve the contingency until the integrity is re-established.

The scenario adopted very simple rules of engagement: ROEs for Blue Force include detecting and discouraging, not use of lethal force, engaging under approval by HQs, reacting to fire, free engagement; while the ROEs for the submarine include hiding, avoiding contact, reacting to fire, engaging at his will; the ROE are directed by the IA-CGF (Bruzzone, Tremori, Massei 2011); the authors conducted V&V (Verification and Validation) on the consistency of ROE application respect different conditions by adopting a testing plan (Bruzzone and Massei 2007; Bruzzone et al. 2002).

The user is entitled to activate the different types of cyber-attacks as well as to change resilience and effectiveness of defensive and offensive actions in cyberspace; in similar way the capabilities of the sensor and assets could be changed by the authors.

The simulation is currently a stochastic hybrid agent driven simulation; stochastic factors include simplified model for communications over the network, failures, success rate and duration of cyber action, detection probabilities and hitting probability, damages, etc.

The communications over the heterogeneous networks are modeled taking into account aspects of reliability and latency affecting both nodes and links, independently from the cyber actions, in order to reproduce the characteristics of the channel (i.e. high latency and disruptions of acoustic underwater comms), but also malfunctions and degenerative operational modes of the ICT (Bruzzone; De Felice et al. 2010); for instance these issues were investigated with non-traditional protocols for underwater communications in heterogeneous networks of AUVs (Merani et al. 2011). It was critical to identify measure of merits in order to compare experimental analysis obtained by MCWS; in this scenario the target functions used to measure the performance have been defined based on desired end state during each single simulation run and are classified in the following 4 classes:

- Sub Success: the submarine successfully passes through the area and reaches East side.
- BF Success: the submarine is detected and tracked successfully and the Blue Force assets reach the condition to be ready to proceed with engagement, blue force stops to act and the submarine resign.
- Sub Down: the submarine is engaged and disabled by Blue Force
- Ship Down: the destroyer is engaged and disabled by the submarine

The scenario was played over the following different hypotheses:

- Limited Scenario: Operations stops when Blue Force is ready to engage the submarine
- Full Operational Scenario: Operations proceed under NATO Art.5 environment
- No Cyber warfare: Cyber Warfare actions are disabled
- Regular Cyber warfare: Cyber Warfare actions are enabled and intensity is set on regular values
- Intense Cyber warfare: Cyber Warfare actions are enabled and intensity is set on high values

It is evident how Cyber Warfare settings are subjected to author hypotheses as well as other parameters; so the experimental results are characterized as relative values (one respect the other ones) much more than as absolute evaluations.

Considering the stochastic nature of the simulator it was necessary to apply ANOVA (Analysis of Variance) in order to estimate the experimental error and confidence bands in the different conditions.

$$\overline{BFS}_{Rate}(k) = \frac{\sum_{i=1}^{k} BE_{ES}(i)}{k} \quad (1)$$

$$MSpE_{BFS_{Rate}}(k) = \frac{\sum_{i=1}^{k} [BE_{ES}(i) - \overline{BFS}_{Rate}(k)]^2}{k-1} \quad (2)$$

$$CF_{BFS_{Rate}}(k) = \frac{1}{2} t_{\alpha,k-1} \sqrt{MSpE_{BFS_{Rate}}(k)} \qquad (3)$$

$$BE_{ES}(i) = \begin{cases} 0 & if\ end\ state\ of\ i-th\ run\ is\ Ship\ Down \\ 0 & if\ end\ state\ of\ i-th\ run\ is\ Sub\ Success \\ 1 & if\ end\ state\ of\ i-th\ run\ is\ Blue\ Force\ Success \\ 1 & if\ end\ state\ of\ i-th\ run\ is\ sub\ down \end{cases}$$

$\overline{\text{BFS}}_{\text{Rate}}$ (k)	Blue Force Success Rate (BFS Rate) after k replications
$BE_{ES}(i)$	Blue Force in End State of the i-th run
n	total simulation replications changing pseudo random seed
k	k-th replication among simulation runs
$MSpE_{BFSRate}(k)$	Mean Square pure Error of BFS Rate after k replications
$CB_{BFSRate}(k)$	Semi amplitude of the Confidence Ban of BFS Rate after k replications
$t_{a,\nu}$	t-Student Distribution with α confidence level and ν degree of freedom

MCWS general architecture is designed in order to federate different models into an interoperable simulation environment; therefore in this case it was implemented within as basic demonstrator and it was used to conduct standalone fast time experiments by using simplified meta-models for sensors and communications.

Such experiments are carried out after defining a specific relevant scenario in order to restrict the range of investigation and test the research most important concepts versus interesting target functions. Indeed, thanks to the experimentation activity, it is possible to evaluate system performance and sensitivity on measure of merits referred to procedures, policies, architectures and technological alternative solution; in the following figures it is proposed only the analysis of the Mean Square pure Error over the different scenario hypotheses (see figure 5, 6, 7 and 8) and a basic comparison of the overall results (figure 9).

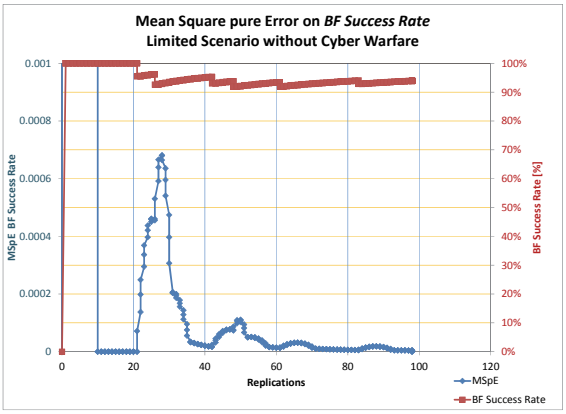

Figure 5: MSpE and Mean BF Success in Limited Scenario without Cyber Warfare

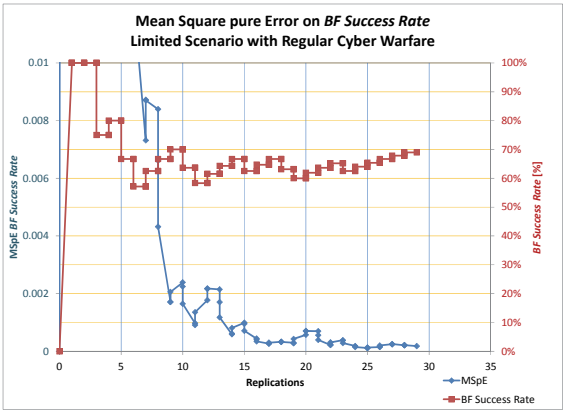

Figure 6: MSpE and Mean BF Success in Limited Scenario with Regular Cyber Warfare

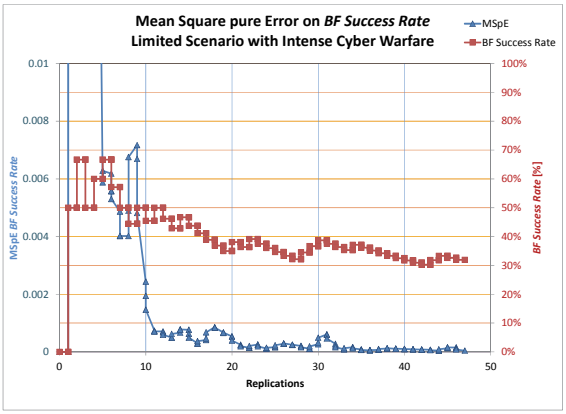

Figure 7: MSpE and Mean BF Success in Limited Scenario with Intense Cyber Warfare

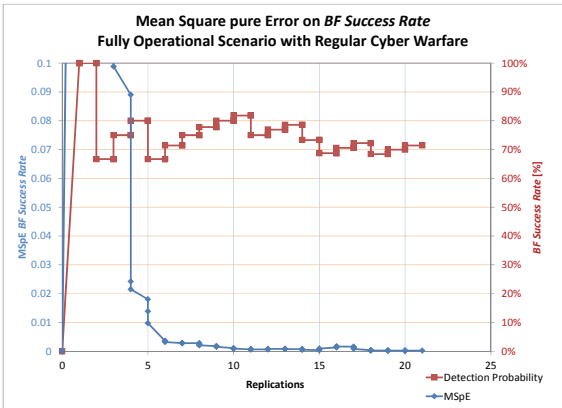

Figure 8: MSpE and Mean BF Success in Fully Operational Scenario with Regular Cyber Warfare

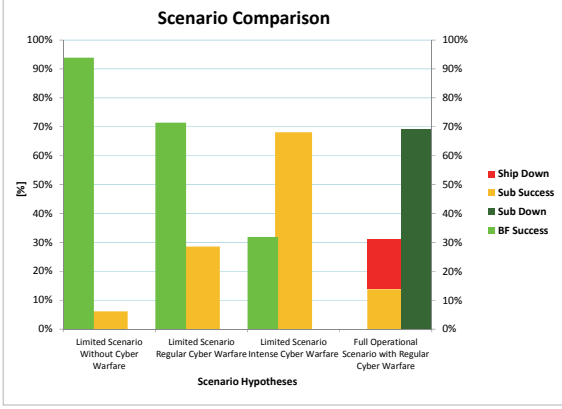

Figure 9: Result comparisons over different hypotheses respect the different end states

From the analysis it emerges the optimal number of replications for each combination of scenario hypotheses; the MSpE and consequently the confidence band results pretty good even with a limited number of replications;
In figure 9 it is proposed the comparison among the different results changing the scenario hypothesis; the analysis confirm the impact of cyber warfare on the Blue Force Success Rate; the *Fully Operational Scenario* produces just a smoothly change respect *Limited Scenario* as expected, considering the additional, even if limited, probability for the submarine to succeed in a confrontation against the Destroyer after successfully being detected and tracked.

6 CONCLUSIONS

The general architecture and conceptual models proposed in the paper were successfully implemented in MCWS simulator focused on a specific basic scenario, inspired to a collaborative ASW mission "hold at risk/secure friendly maneuver area", conducted via autonomous underwater vehicles; therefore even the case study proposed represent a relevant mission environment respect existing research and available models; the results obtained are very interesting and the potential of this approach by the interoperability with other models is very great providing scalable solution to complex scenarios; indeed the described approach is open to be extended and applied to more sophisticated context.
The use of MCWS allows conducting experimental analysis; by this approach, it is possible to use sensitivity analysis in order to evaluate the most influent parameters, the second and high order effects, and to quantify the degree of uncertainty as well as the experimental error (Montgomery 2000); the simulation allows to test criteria to identify emergent behaviors and to estimate risk to violate or to compromise cyber resources; preventive action efficiency, mitigation procedures and reactions are tested and evaluated in terms of their impact on the operational scenario through simulation experiments; indeed the quantitative experimentation proposed in this paper confirms the benefits of the proposed approach and the importance of adopting simulation as investigation aid for cyber warfare within operational frameworks.

REFERENCES

Affenzeller M., S. M. Winkler, S. Wagner, A. Beham (2009) "Genetic Algorithms and Genetic Programming" CRC Press (Taylor & Francis Group)

Baiardi F., Telmon C., Sgandurra G. (2012) "Haruspex—Simulation-driven Risk Analysis for Complex Systems", JournalISACA Volume 3

Bruzzone A.G. (2013) "New Challenges for Modelling & Simulation in Maritime Domain", Keynote Speech at SpringSim2013, San Diego, CA, April

Bruzzone A.G., Berni A., Fontaine J.G., Brizzolara S., Longo F., Poggi S., Dallorto M., Dato L., (2013) "Simulating the Marine Domain as an Extended Framework for Joint Collaboration and Competition among Autonomous Systems ", Proceedings of I3M2013, Athens, September

Bruzzone, A.G., Tremori, A., Massei, M., (2011) "Adding Smart to the Mix," Modeling, Simulation & Training: the International Defence Training Journal, 3, 25-27.

Bruzzone, A.G., Massei, M., Tremori, A., Longo, F., Madeo, F., Tarone, F. (2011) "Maritime security: emerging technologies for asymmetric

threats." In Proceedings of the European Modeling and Simulation Symposium, EMSS2011 (Rome, Italy, September 12-14).

Bruzzone A.G., Massei M., Tarone F., Madeo F. (2011) "Integrating Intelligent Agents & AHP in a Complex System Simulation", Proceedings of the international Symposium on the AHP, Sorrento, Italy, June.

Bruzzone A.G. (2010) "Project Piovra on Intelligent Agents and CGF", Technical Report for A-03-IT-1682 Italy USA M&S Data Exchange Agreement, November 4-5

Bruzzone A.G. (2008) "Intelligent Agents for Computer Generated Forces", Invited Speech at Gesi User Workshop, Wien, Italy, October 16-17

Bruzzone A.G., Massei M. (2007) "Polyfunctional Intelligent Operational Virtual Reality Agent: PIOVRA Final Report", EDA Technical Report

Bruzzone A.G., Frydman C., Junco S., Dauphin-Panguy G. (2005) "International Mediterranean Modelling Multiconfernece - International Conference on Integrated Modelling and Analysis in Applied Control and Automation", LSIS Press, ISBN 2-9520712-5-X (pp 194)

Bruzzone, A.G. et al. (2002) "Simulation -based VV&A methodology for HLA federations: an example from the Aerospace Industry", Proceedings of 35th Annual Simulation Symposium, vol., no. , pp.80,85, April

Bruzzone A.G., E.Page, A.Uhrmacher (1999) "Web-based Modelling & Simulation", SCS International, San Francisco, ISBN 1-56555-156-7

Bruzzone A.G., Giribone P. (1998) "Decision-Support Systems and Simulation for Logistics: Moving Forward for a Distributed, Real-Time, Interactive Simulation Environment", Proceedings of the 31st Annual Simulation Symposium, Boston MA, April

Calfee, S.H., Rowe, N.C., 2004. "Multi-agent simulation of human behavior in naval air defense," Naval Engineers Journal, 116, no.4, 53-64.

Cornforth D., Kirley M., Bossomaier T. (2004) "Agent Heterogeneity and Coalition Formation: Investigating Market-Based Cooperative Problem Solving", AAMAS: 556-563

De Felice F., G. Di Bona, D. Falcone, A. Silvestri (2010) "New Reliability allocation methodology: the Integrated Factors Method", International Journal of Operations & Quantitative Management Volume 16 Number 1, ISSN: 1082-1910

Feddema, J.T.; Lewis, C.; Schoenwald, D.A., "Decentralized control of cooperative robotic vehicles: theory and application, "Robotics and Automation, IEEE Transactions on, vol.18, no.5, pp.852,864, Oct 2002

Hua Guo, Fei Tao, Lin Zhang, Suyi Su, Nan Si (2010) "Correlation-aware web services composition and QoS computation model in virtual enterprise", International Journal of Advanced Manufacturing Technology, 51, 5-8 , 817-827.

Jakobson, G., Lewis, L., Buford, J., Sherman, C.E. (2004) "Importance of Considering Future War as a Convergence of Real and Cyber Battlespaces - Battlespace situation analysis: the dynamic CBR approach", Military Communications Conference, MILCOM IEEE, Vol. 2 Page(s): 941 - 947

Kalra N., D. Ferguson and A. Stentz: A generalized framework for solving tightly-coupled multirobot planning problems, Proc. of the IEEE International Conference on Robotics and Automation, April 2007, pp.3359-3364. Kennedy, K.P., 2010. "Training: the key to keeping your head in a crisis situation," Naval Engineers Journal, 122, no.3, 73-85.

Kotenko, I. (2007) "Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security" Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2007. 4th IEEE Workshop

Kuhl, F., Weatherly, R., Dahmann, J., 1999. Creating Computer Simulation Systems: An Introduction to the High Level Architecture. Prentice Hall, Upper Saddle River, USA.

Longo, F., Bruzzone, A.G. (2005) "Modelling and Simulation applied to Security Systems". Proceedings of Summer Computer Simulation Conference, pp. 183-188

Martins, R.; de Sousa, J.B.; Afonso, C.C.; Incze, M.L., "REP10 AUV: Shallow water operations with heterogeneous autonomous vehicles," OCEANS, 2011 IEEE - Spain, vol., no., pp.1,6, 6-9 June 2011

Massei, M., Tremori, A., 2010. "Mobile training solutions based on ST_VP: an HLA virtual simulation for training and virtual prototyping within ports." In Proceedings of the 2010 International Workshop on Applied Modeling and Simulation, WAMS2010 (Buzios, Brazil, May 5-7).

Merkuriev Y., Bruzzone A.G., Novitsky L (1998) "Modelling and Simulation within a Maritime

Environment", SCS Europe, Ghent, Belgium, ISBN 1-56555-132-X
Montgomery D.C. (2000) "Design and Analysis of Experiments", John Wiley & Sons, New York
Nad, D., Miskovic, N., Djapic, V., Vukic, Z. (2011) "Sonar aided navigation and control of small UUVs",Proceeedings of the 19th Mediterranean Conference on Control & Automation (MED), Corfu, Greece, June
Nabil Adam, Randy Stiles, Andrew Zimdars, Ryan Timmons, Jackie Leung, Greg Stachnick, Jeff Merrick, Robert Coop, Vadim Slavin, Tanya Kruglikov, John Galmiche, and Sharad Mehrotra. (2013) "Consequence analysis of complex events on critical U.S. infrastructure". Commun. ACM 56, 6 (June 2013), 83-91.
Massei M., Tremori A., Poggi S., Nicoletti L., (2013) "HLA based real time Distributed Simulation of a Marine Port for Training Purposes", International Journal of Simulation and Process Modeling, Vol.8, No.1, pp.42-51
Merani, D., Berni, A., Potter, J., Martins, R. (2011) "An Underwater Convergence Layer for Disruption Tolerant Networking", Proceeedings of Baltic Congress on Future Internet Communications, Riga Feb. 16-18
Ören, T.I. and L. Yilmaz (2009) "On the Synergy of Simulation and Agents: An Innovation Paradigm Perspective", Special Issue on Agent-Directed Simulation. The International Journal of Intelligent Control and Systems (IJICS), Vol. 14, Nb. 1, March, 4-19.
Rumekasten, M. , (1994) "Simulation of Heterogeneous Networks", Proceedings Winter Simulation Conference, pp. 1264 - 1271
Sujit, P. B.; Sousa, J.; Pereira, F.L., "UAV and AUVs coordination for ocean exploration,"OCEANS 2009 - EUROPE, vol., no., pp.1,7, 11-14 May 2009
Tanner H.G., D.K. Christodoulakis, Decentralized cooperative control of heterogeneous vehicle groups, Robotics and Autonomous Systems 55 (2007) 811–823
Tether, T. (2009) "Darpa Strategic Plan", Technical Report DARPA, May
Thompson J., Bossomaier T. (2006) Agent Based Modelling of Coevolution of Trust between Client and Wealth Managers", CIMCA/IAWTIC, 131
Vail D. and M. Veloso: Dynamic multi-robot coordination, In Multi-Robot Systems: From Swarms to Intelligent Automata, Vol II, 2003, pp. 87-100.
Wiedemann J. (2013) "Naval Forces", Special Issue 2013, Vol.XXXIV ISSN 0722-8880
Zacharewicz G., Frydman C., Giambiasi N. (2008) "G-DEVS/HLA Environment for Distributed Simulations of Workflows", Simulation, Vol.84, N.5, pp 197-213
Zini A. (2012) "Virtual Ship: Dream or Reality", Keynote Speech at Summersim 2012, Genoa, July
"Methodology for analyzing the compromise of a deployed tactical network", Asman, B.C. ; Kim, M.H. ; Moschitto, R.A. ; Stauffer, J.C. ; Huddleston, S.H., Systems and Information Engineering Design Symposium (SIEDS), 2011 IEEE Digital Object Identifier: 10.1109/SIEDS.2011.5876871 Publication Year: 2011 , Page(s): 164 - 169
Urias, V. ; Van Leeuwen, B. ; Richardson, B. (2012) "Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed" MILITARY COMMUNICATIONS CONFERENCE- MILCOM Digital Object Identifier: 10.1109/MILCOM.2012.6415818 Publication Year: 2012 , Page(s): 1 - 8

WEB REFERENCES

- http://www.cmre.nato.int
- http://www.itim.unige.it
- http://www.liophant.org/projects/ia_cgf_ucoin.html
- http://www.mastsrl.eu/solutions/ia_cgf_t4.html
- http://www.simulationteam.com