MODELLING OF IMMUNE FUNCTIONS IN A WIRELESS SENSORS NETWORK

Jan Nikodem [(a)], Ryszard Klempous[(a)], Zenon Chaczko[(b)]

[(a)]Wroclaw University of Technology, Poland
[(b)]University of Technology Sydney, NSW, Australia

[(a)] Jan.Nikodem@pwr.wroc.pl, [(b)] Ryszard.Klempous@pwr.wroc.pl, [(c)] Zenon.Chaczko@uts.edu.au

ABSTRACT
In this paper we explore relationships between immunity and adaptation in Wireless Sensors Network (WSN). We consider the WSN as a set of sensors deployed in a given area. The sensors must communicate to achieve both their particular self-interests and global goals. In the proposed approach we determine immunity and adaptation abstractions and considering them in the context of three fundamental relations (subordination, tolerance, collision). The proposed conceptual framework provides a powerful paradigm to conceptualise, model, support and manage dynamically organizing complex systems processes.

Keywords: artificial immune system, immunity of WSN, relations in complex system

1. INTRODUCTION

The research presented in this paper aims to focus on the Wireless Sensors Network (WSN) that consists of homogeneous sensors cooperating with each other. WSN is not organised centrally, but rather in a distributed manner.

Each individual sensor has limited resources such as: energy, hardware, software and communication range, hence in the individual level it is not able to realise overall system tasks. Due to these limitation, sensors are required to lesser or greater degree strictly follow an integrated cooperation between them. This activity is realised predominately in the information domain, as it is essential for the WSN dependability to provide a robust communication capability.

From one point of view, each sensor works in its precinct (vicinity) autonomously, interacting with environment stimulus; And from the other point of view, sensors must communicate with each other, therefore communication channels are crucial elements of the WSN architecture. In general, sensors are simple, unsophisticated technical components performing tasks determined by programmers and engineers. Because of that the risk of unauthorized access or even a possible destruction of communication links by outsiders can be an increasing threat. External attackers are often responsible for causing communication and routing disruptions including the breach of security. Frequently, however, it is the internal events which may contribute to serious decrease in efficiency of communication channels.

2. BASIC IDEAS AND RATIONALE

When describing the WSN activity we will be discussing the concepts of actions and behaviour. Action should be considered the property of every network element such as: a sensor, a cluster head or a node. The Behaviour, on the other hand is an external attribute which can be considered either as an outcome of actions performed by the whole WSN or its subset (i.e. cluster, tree, sensor field, vicinity). *Action* is a ternary relation which can be defined as follows:

$$Act : Nodes \times State \rightarrow State. \tag{1}$$

Based on this we can construct the quotient set *Behaviour*, elements of which are called equivalence classes linked to the relation *R* and here denoted as:

$$Beh : Act / R = \{act \in Act \mid act\ R\ x\}. \tag{2}$$

2.1. Neighbourhood abstraction

Let us define *Map(X, Y)* as a set of mapping functions from *X* onto *Y* (surjection). Where *Sub(X)* is defined as a family of all *X* subsets. We define the neighbourhood $\mathcal{N}$ as follows:

$$\mathcal{N} \in Map(Nodes, Sub(Nodes)). \tag{3}$$

Thus, $\mathcal{N}(k)$ is the neighbourhood of node *k*, and $\mathcal{N}(C)$ is the neighbourhood of *C* (set of nodes) defined below as:

$$\mathcal{N}(k)\big|_{k \in Nodes} := \{y \in Nodes \mid y R_{\mathcal{N}} k\}, \tag{4}$$

$$\mathcal{N}(C)\big|_{C \subset Nodes} := \{y \in Nodes \mid (\exists x \in C)(y R_{\mathcal{N}} x)\}. \tag{5}$$

The formal view emerging from the above discussion will project a construction of the extended WSN behavioural model and related to the challenges of individual tasks versus collective activities of network elements. By *Individual* it is meant that the node/sensor improves its goal-reaching activity,

interacting with its neighbourhood $\mathcal{N}(k)$ while collective activity relates to $\mathcal{N}(C)$ neighbourhood.

2.2. Relational attempt to network activity

In 1978 J. Jaron has developed an original methodology for the systemic cybernetics (Jaron 1978) which describes three basic relations between systems components such as: subordination (π), tolerance (ϑ) and collision (χ). We find these basic relations very useful in describing activities and qualitative relations between components of the WSN. For concepts presented in this paper, and for discussion on the immune functions in communication activities, we require to refer the following three key relations:

$$\pi := \{< x, y >; x, y \in Act \,|\, x \pi y\}. \tag{6}$$

The expression $x \ \pi \ y$ - defines the action x which is subordinated to the action y or action y dominate over action x.

$$\vartheta := \{< x, y >; x, y \in Act \,|\, x \vartheta y\}. \tag{7}$$

The expression $x \vartheta y$ - states that the actions x and y tolerate each other,

$$\chi := \{< x, y >; x, y \in Act \,|\, x \chi y\}. \tag{8}$$

And finally $x\chi \ y$ - means the actions x and y are in collision to one another. The basic properties of mentioned above relations could be formulated succinctly as follows (Jaron, 1978):

$$\pi \cup \vartheta \cup \chi \subset Act \times Act \neq \emptyset, \tag{9}$$

$$\iota \cup (\pi \cdot \pi) \subset \pi, \tag{10}$$

where $\iota \subset Act \times Act$ is the identity on the set *Action*.
Moreover,

$$\pi \cup \vartheta^{-1} \cup (\vartheta \cdot \pi) \subset \vartheta, \tag{11}$$

where ϑ^{-1} is the converse of ϑ so,

$$\vartheta^{-1} := \{< x, y > \in X \times Y \,|\, y \vartheta x\}. \tag{12}$$

For collision,

$$\chi^{-1} \cup (\pi \cdot \chi) \subset \chi \subset \vartheta'. \tag{13}$$

where ϑ' is the complement of ϑ so,

$$\vartheta' := \{< x, y > \in X \times Y \,|\, < x, y > \notin \vartheta\}. \tag{14}$$

The formula (9) indicates that all these three relations are binary on nonempty set *Actions*. The formula (10) describes fundamental properties of subordination relation which is reflexive and transitive. Therefore it is also ordering relation on the set *Actions*.

The formula (11) states that subordination implies the tolerance. Hence we can obtain:

$$(\forall x, y \in Act)(x \pi y \Rightarrow x \vartheta y) \tag{15}$$

and subordinated actions must tolerate all actions tolerated by dominants

$$(\forall x, y, z \in Act)((x \pi y \wedge y \vartheta z) \Rightarrow x \vartheta z). \tag{16}$$

3. MODELLING OF IMMUNE FUNCTION

Immunity is the distributed rather than the global property of a complex system. The complexity of the immune function, the absence of simple feedback loops, a high complexity of tasks and activities; and collective (not central) rather than individual regulatory processes all results in serious challenges for attempts to define system's immune competences.

There are a number of fundamental works corresponding to this domain and related to artificial systems (Hofmeyr, Forrest, 2000), (Timmis, 2000). Some authors have drawn inspiration from the biological immune system, incorporated a lot of properties from autonomous immune systems.

In this article, we propose a novel relational approach to modelling of the system immunity. In our attempt we are considering the immunity not as a set of particular mechanisms like clonal selection, affinity maturation or elements (antigens, antibodies, idiotopes, paratopes, etc.). In the proposed approach the phenomenon of immunity appears to be a result of inter-relations among members of community (neighbourhood).

Let us consider for the node k, its neighbourhood $\mathcal{N}(k)$. Any communication activity act_k that is performed by node k relates to some members of $\mathcal{N}(k)$ and the set of actions act_k within neighbourhood $\mathcal{N}(k)$ can be defined as follows:

$$Act_{\mathcal{N}}(k) := \{act_k \in Act \,|\, (\exists x \in \mathcal{N}(k))(act_x R act_k)\}. \tag{17}$$

If n is a number of actions act_k within neighbourhood $\mathcal{N}(k)$, then it can be expressed as cardinality *Card* $(Act_{\mathcal{N}}(k))$. The collection of all subsets of $Act_{\mathcal{N}}(k)$ is determined as power set $Pow(Act_{\mathcal{N}}(k))$ with cardinality 2^n. Finally, any subset of that power set is called a family *Fam* $(Act_{\mathcal{N}}(k))$ of communication activity within neighbourhood $\mathcal{N}(k)$.

The Cartesian product defined as:

$$IS_k := Act_{\mathcal{N}}(k) \times Act_{\mathcal{N}}(k) \subseteq \pi \cup \vartheta \cup \chi \tag{18}$$

describes interaction space IS_k within $\mathcal{N}(k)$.

Let us now consider z_k=Card(IS_k) which defines a number of possible interactions within neighbourhood N(k) which can be expressed as:

$$R_k := \{ y \in Act_{\mathcal{N}}(k) \mid < k, y > \in IS_k \wedge kRy \}. \quad (19)$$

Thus, for a given relation R we define intensity quotient within neighbourhood $\mathcal{N}$(k) as follows:

$$IR_k = Card(R_k) / z_k. \quad (20)$$

The rationale behind our choice of the relational approach to modelling immune functions is the fact that interactions are factual and a very relevant aspect of elements of the immune system. The immune system itself can be defined as a very large complex network with a layered and hierarchical architecture. Relationships between components of this architecture can be described by the subordination relations (π). Furthermore, a positive response of the immune functions would result from the collision relation (χ) while a negative response would be attributed to tolerance (ϑ) relation.

An immune system is adaptive in nature in the sense that its positive or negative responses should be adequate to environment stimulus. Since resources are limited, the allocation rule predicts that an increased investment in system adaptability will come at a cost to investment in immunity (and vice versa). Growing adaptability decreasing system immunity and extends possibility of adversary's attacks. On the other hand, growing immunity barrier tends to adaptability reduction. Bellow we define immunity and adaptability as follows;

$$immun := \{ < x, y >; y, x \in Act \mid < x, y > \in \vartheta' \cup \chi \}, \quad (21)$$

$$adapt := \{ < x, y >; y, x \in Act \mid < x, y > \in \vartheta \cup \pi \}. \quad (22)$$

Therefore, the scope of immunity is determined by decreasing tolerance and growing collision relations when the extend of adaptation is determined by expanding tolerance and subordination.

Additionally, based on (21), (22) it is possible to model adaptation - immunity characteristics of a system and consider it as a process of finding a fine homeostatic balance between them. In our case the set of feasible solutions is modelled as a line segment (Figure 1) linking strong immunity *(SI)* and strong adaptability *(SA).* This line is obtained as the intersection of a plane [*SA*, (1,1,0), *SI*, (0,0,1)] with a plane [(0,0,0), *SI*, (1,1,1), *SA*)]. In such approach it is practically impossible to determine balance point $B \in$ *(SI; SA)* which corresponds to both global and any local situations. Based on relational approach (21), (22), it is evident (as shown in Figure 1) that the issues of keeping the balance between adaptation and immunity is far more refined then simply finding a point on line segment *(SI; SA).* This line segment is a canonical projection of topological space subset (tetrahedral on Figure1). Any point at this solid figure represents one of

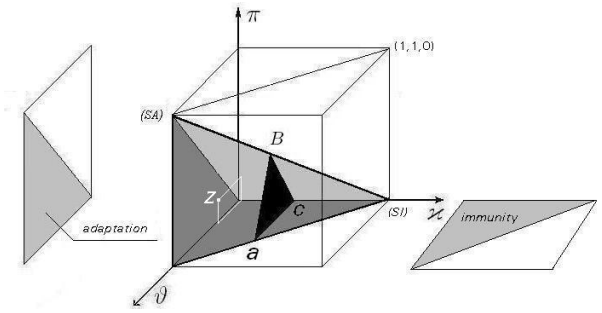


Figure 1: Modelling immunity based on π, ϑ and χ relations.

many, feasible solution which can fulfil (for better or worse) the quality requirements of the network system.

Choosing the point $B \in$ *(SI; SA)* we determine globally the desirable adaptability/immunity homeostatics. However, for each node, owing to its neighbourhood state, it is necessary to determine an individual point of balance. The set of such points has to be determined with reference to equivalent class (triangle *aBc* in Figure 1) that corresponds exactly to one point *B* (Figure 1) on a line segment *(SI; SA).*

4. HOW IT WORKS IN PRACTICE

In order to illustrate the modelling immunity result with a concrete model simulation, consider WSN with 10 nodes and one base station (BS). To determine neighbourhood $\mathcal{N}(k)$ assignment we use radio link range. Therefore, coming back to the (3)-(4) we create subsets $\mathcal{N}(k)$, *k=1, 2.., 10.* Each cell *n* of row *k* in the binary matrix $\mathcal{N}$ (Figure 4) represents a membership $n \in \mathcal{N}(k)$. It is worth mentioning that a neighbourhood always related to communication range, but very rare corresponds with a structure of clusters. Such constructed neighbourhood subsets are unambiguous and stable as long as a communication range is fixed.

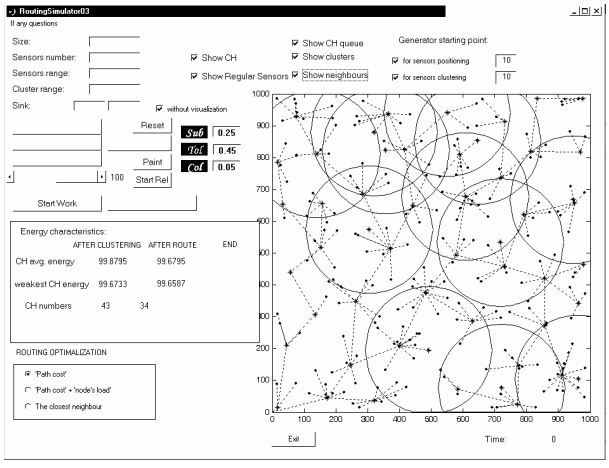


Figure 2: WNS activity simulator based on relational space (π, ϑ and χ relations).

In the context of WSN activity, we focus our attention on routing aspects. Therefore in furthers consideration, from all action sets $Act_{\mathcal{N}}(k)$ within neighbourhood k we select only these, performed routing activity. In such way we obtain a family *Fam* ($Act_{\mathcal{N}}(k)$) of routing activity. Considering the distance from the base station (BS) to a node position, a routing activity within $\mathcal{N}(k)$ is partially ordered ($\leq$). Additional preferences were given to cluster heads (CH) and those nodes which belong to routing tree. Firstly, a cluster heads on routing path are the nearest BS, next another BS, finally the other nodes within $\mathcal{N}(k)$ (Figure 3).

In order for us to proceed any further, it is necessary to combine the WSN spatial structure (topology) and the WSN activity. To facilitate this process we are required to construct a product that describes the interaction space IS_k within $\mathcal{N}(k)$ as defined in (18). Each element of the interaction space (regardless of which neighbourhood we consider), according to the right side of (18) equation is mapping (as a point) to (may be not injection) the 3D relational space [π, ϑ, χ] as presented in Figure.1 above.

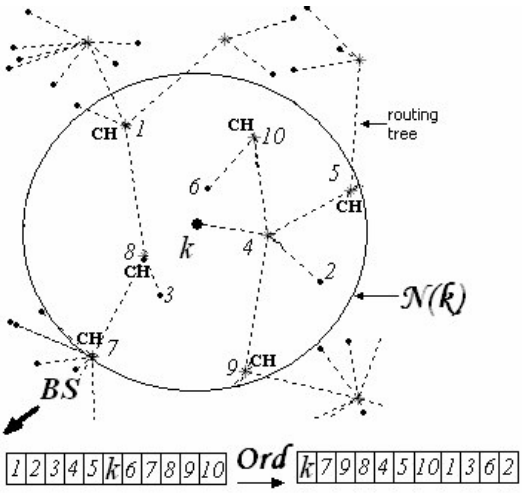


Figure 3: Modelling partially ordered neighbourhood abstraction $\mathcal{N}(k)$.

In order to model [π, ϑ, χ] space we exploit three additional matrices presented on Figure 4. The real number in any cell of these matrices expresses an intensity quotient of relation. Elements $[r_{k,k}]$ represent intensity quotient within $\mathcal{N}(k)$, while $[r_{i,j}]$ related to particular *i-j* nodes interactions. Henceforth, we are ready to model the dichotomies of the WSN characteristics - immunity and adaptability.

The initial step is the determination of the global (for whole network) strategy GS_{WSN} for the network activity. For this aim, we construct a subset of relational space (9) as a conjunction of (10), (11), (13) with (21), (22). This subset (depicted as tetrahedral in Figure 1) consists of all feasible actions. The derived set constitutes a global interaction space IS_{WSN} (18) within the WSN network. Now we shall determine global strategy GS_{WSN} as a subset of interaction space IS_{WSN}. Notice that there are a huge number of different choices of such subset, but for simplicity reason we consider only two. First is the subset:

$$GS^1_{WSN} = \{ y \in IS_{WSN} \,|\, y \in \Delta aBc \}, \tag{23}$$

where, ΔaBc - is a black triangle on Figure1, second is a white point Z on the same Figure 1. While first is a restriction from 3D to 2D, the second is restriction from 3D to 1D mapping. Clearly, any restriction of IS_{WSN} space offers less choices then the whole, but as we have shown bellow even in case of singleton

$$\{Z\} = \{\langle \pi_k, \vartheta_k, \chi_k \rangle\} = \{\langle 0.2, 0.54, 0.07 \rangle\} = GS^2_{WSN} \tag{24}$$

the spectrum of possible activities is rather wide.

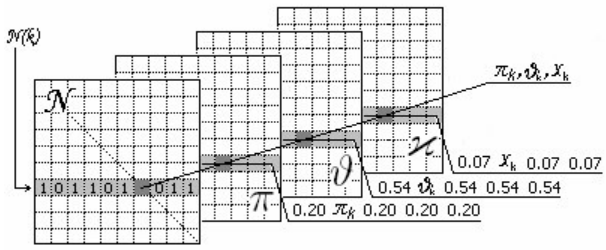
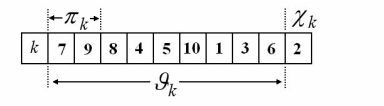


Figure 4: Modelling relational (π, ϑ, χ) space within $\mathcal{N}(k)$ neighbourhoods.

In the following step we shall determine local strategy for each neighbourhood $\mathcal{N}(k)$, $k=1, 2.., 10$. In order to deal with the case where the global strategy is determined by (24) the local strategy for neighbourhood activity need to be identical. Hence for each node k its interaction space IS_k is a singleton $\{Z\}=\{<\pi_k, \vartheta_k, \chi_k>\}$ exactly the same like (24) and the real numbers π_k, ϑ_k, χ_k occupied main diagonal cells of relational matrices π, ϑ, χ (Figure 4). Henceforth, the proper local (within neighbourhood $\mathcal{N}$(k)), activity can be accomplished in accordance with the global strategy. Thereby, instead to force the local activity of each node, we are rather formulating requirements for the nature and intensity of relations within $\mathcal{N}$(k)). Fulfilment of these requirements results in desired global strategy.

In the last step of preparing the simulation process we shall determine non-diagonal elements of relational matrices (Figure 4). To facilitate the representation of nodes interactions (point-to-point) we assign them a real numbers exactly the same like on diagonal. The starting point of simulation determined in such way is feasible of course (holds both local and global strategies).

The relational state for any $\mathcal{N}$(k) is now identified with ordered sequence of node indexes as follows:



$$\langle \pi_k , \vartheta_k , \chi_k \rangle = \langle 0.2, 0.54, 0.07 \rangle. \quad (25)$$

Considering that a given WSN consists of 10 nodes, we say there is ten different ordered sequences, which all together constitute the WSN relational state.

In each iteration, we choose randomly both the sender *s* (node sending information to BS) and a position in the relational space $\mathcal{N}(s)$. It determines the next-hop path forwards to BS (the receiver node) and type of relation describing this hop. In the following, for chosen receiver *r*, we will make a decision taking into account relational state for *sender-receiver* interaction (cells $\pi_{s,r}$, $\vartheta_{s,r}$, $\chi_{s,r}$). Accordingly to obtained results we modify the intensity quotients for *sender-receiver* interaction and repeat hops until information reaches the base station.

Modelling WSN lifetime activity we modify repeatedly matrices π, ϑ, χ, but diagonal elements remains the same. It is apparent that the spatial distribution of intensity quotients fulfils global requirements, but is has captured the essential local relationships within any neighbourhood.

Described above method meets other important requirements for immunity and adaptability. The interaction space within $\mathcal{N}(k)$ shall be modified only in the local vicinity of each node *k* and that all the modified interaction spaces shall then resemble the prevailing activity better then before. They tend to become more similar mutually i.e. differences between any interaction spaces within $\mathcal{N}(C)$ (where $k \in C$) are smoothed.

5. CONCLUSIONS

Dependability of a complex distributed system closely depends on its immunity and adaptation abilities for data exchange. Immunity and adaptation of communication channels are essential in our approach.

We propose a novel relational method which allows reconciling two often dichotomous points of view: immunity and adaptability to neighbourhood. The global network strategy provides each node with an adequate level of immunity and adaptation functions thus guaranteeing sufficient communication services.

On the other hand, nodes using these resources provide suitable level of the WSN adaptability and immunity towards the desired common network security level. Such management of complex system yields in growing both system adaptability and immunity.

By modelling WSN activities using relational approach we have managed to accurately describe the complex characteristics of the network interactions, and at the same time we have eliminated many different and distributed variables (the WSN parameters). This reduction can be crucial for system simulation. Hence, with the presented relational approach for modelling immunity functions we are able to scale the complexity of interactions and model with much higher precision various behavioural aspects of WSNs.

REFERENCES

Cohn, A.G., Bennett B., Gooday J.M., Gotts N.M., 1997. Representing and Reasoning with Qalitative Spatial Relations about Regions. In: Cohn, A.G., Bennett B., Gooday J.M., Gotts N.M, eds. *Spatial and Temporal Reasoning*, Dordrecht, Kulwer, 97-134.

Dasgupta D., Immunity-based Intrusion Detection System: A General Framework. Proceedings of the Conference in *22th International Information System Security Conference,* 18-21, Oct. 1999.

Hofmeyr, S., Forrest, S. 2000. Architecture for an Artificial Immune System. *Evolutionary Computation,* vol.8, no.4: 443-473.

Jaron J., 1978. Systemic Prolegomena to Theoretical Cybernetics, *Scientific. Papers of Institute of Technical Cybernetics*, no. 45, Wroclaw University of Technology.

Jungwon, K.,Bentley, P. 2001. Towards an artificial immune system for network intrusiondetection: an investigation of clonal selection with a negativeselection operator, Proceedings of the Conference in *2001 Congress on Evolutionary Computation,* vol.2, 1244-1252. 27-30 May 2001, Seoul, South Korea

Kohonen T., 2001. *Self Organizing Maps*, Springer Series in Information Science, no. 30, Springer-Verlag, Berlin-New York.

Leandro N. de Castro and Jon Timmis. 2002. *Artificial Immune Systems: A new computational intelligence approach*, Springer-Verlag, Great Britain.

Luther, K., Bye, R., Alpcan, T., Muller, A., Albayrak, S. A. 2007. Cooperative AIS Framework for Intrusion Detection, Proceedings of the Conference in *IEEE International Conference on Communications ICC'07*, 1409 -1416. 24-27 June 2007. Glasgow, Scotland.

Nikodem, J., 2008. Autonomy and Cooperation as Factors of Dependability in Wireless Sensor Network, Proceedings of the Conference in *Dependability of Computer Systems, DepCoS - RELCOMEX 2008*, 406-413. 26-28 June 2008, Szklarska Poreba, Poland.

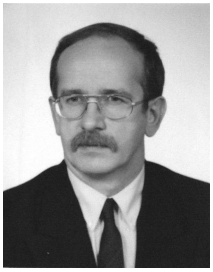
Su P., Feng D., 2006. The Design of an Artificial Immune System, Proceedings of the Conference in *Networking, Systems, Mobile Communications and Learning Technologies (ICNICONSMCL'06)*,

Timmis, J. I.,2000. *Artificial Immune Systems: A novel data analysis technique inspired by the immune network theory*. Ph.D. thesis. Department of Computer Science, University of Wales.

Thomas S., 2006. *On the Appropriateness of Negative Selection for Anomaly Detection and Network*

Intrusion Detection. Ph.D. thesis. Darmstadt University of Technology.

AUTHORS BIOGRAPHY



Jan Nikodem received the B.Sc. in electrical engineering, M.Sc. in artificial intelligence in 1979 and Ph.D. degree in computer science in 1982 from Wroclaw University of Technology (WUT), Poland. Since 1986, he has been an Assistant Professor in the Institute of Technical Cybernetics, WUT. Since 2005 in the Institute of Computer Engineering, Automatics and Robotics (ICEAR). His current research are focused on the area of complex and distributed systems, cybernetics, wireless sensor networks and digital data transmission.

Ryszard Klempous holds a M.Sc. in Automation (1971) and Ph.D. in Computer Science (1980) from Wroclaw University of Technology (WUT). Since 1980 he has been an Assistant Professor in the Institute of Computer Engineering, Automatics and Robotics, WUT. Senior member of IEEE and NYAS, has already published over 90 papers in Optimization Methods and Algorithms, Simulation and Data Processing and Transmission.

Zenon Chaczko completed a B.Sc. in Cybernetics and Informatics in 1980 and a M.Sc. in Economics in 1981 at the University of Economics, Wroclaw in Poland., as well as completed MEng in Control Engineering at the NSWIT 1986, Australia. For over 20 years Mr Chaczko has worked on Sonar and Radar Systems, Simulators, Systems Architecture, Telecommunication network management systems, large distributed Real-Time system architectures, network protocols and system software middleware. Mr Chaczko is a Senior Lecturer in the Information and Communication Group within the Faculty of Engineering at UTS.