Infrastructures protection based on heterogeneous networks

Agostino G. Bruzzone* and Marina Massei

DIME, University of Genoa,
via Opera Pia 15, 16145 Genova, Italy
Email: agostino@itim.unige.it
Email: massei@itim.unige.it
*Corresponding author

Simonluca Poggi

Simulation Team,
University of Genoa,
via A. Magliotto 2, 17100 Savona, Italy
Email: simonluca.poggi@simulationteam.com

Abstract: This paper presents a modelling approach for mapping cyber defence issues with respect to heterogeneous networks; the research is devoted to develop an agent-driven simulation environment able to analyse this problem considering different layers including CIS capabilities, operational issues, system architecture, management processes and human factors. The paper analyses a specific case study to validate and verify the proposed modelling approach; the scenario is focused on a heterogeneous network applied to an 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 defence; interoperable simulation; maritime simulation; modelling and simulation; M&S; heterogeneous networks; autonomous systems.


Biographical notes: Agostino G. Bruzzone is a Full Professor at DIME University of Genoa, Director of M&S Net, Director of the MISS – Genoa Center, Founder and President of the Liophant Simulation, member of the board of MIMOS, and member of the NATO MSG. He works on innovative modelling for a broad spectrum of application (defense, business, oil and gas, logistics). He serves as General Coordinator of Scientific Initiatives (i.e. General Chair of I3M). He teaches M&S for the DIMS PhD program. He is the Director of the Master Program in Industrial Plants. He is Project Leader M&S for NATO Science & Technology Organization at the CMRE.

Marina Massei operates with Prof. Bruzzone’s team at DIME University of Genoa as Project Controller. She participated in the organisation of SIREN Courses (HLA, VV&A, M&S) and IEPAL Meetings. She organised several international scientific events (I3M, SummerSim) and coordinated Technical Councils for Advanced Techniques (SIMPLEST). She served as Chair for Applications in Management, Planning & Forecasting Workshop, SummerSim 2004, 2005, 2006. She is an Associate Director of the McLeod Institute for Simulation Science located at Perugia University. She is currently enrolled in DIME University of Genoa as member of the Simulation Team. She conducted several projects on mobile and virtual simulation.

Simonluca Poggi received his PhD in M&S and Mathematical Engineering from the Genoa University. He works on HB M&S and Intelligent Agents for simulation for training in complex environments. He is actively involved in Virtual HLA Real Time Simulation and edutainment for Marine applications projects. He is a member of the Simulation Team of the University of Genoa, since 2006 he is involved on several projects on customer satisfaction analysis for the retail industry, ERP solutions, inventory management, logistics and project management. He also has knowledge of M&S for defence with special focus on life cycle analysis for new vessels.

Copyright © 2016 Inderscience Enterprises Ltd.
Introduction

The research aims at matching the NATO topology of heterogeneous networks with cyber defence 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 behaviours, environmental conditions, assets reliability, models maturity, agility, node compromised resources, etc. Such increasing popularity is expected to become very common in military fields as a consequence of the technology evolution trends with special attention to autonomous systems, robots and sensor networks (Bruzzone et al., 2005; DARPA, 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 defence issues.

Owing to the high level of interactions among the networks and their complexity, this application field requires to be investigated using modelling and simulation (M&S); indeed the presence of several stochastic factors affecting the behaviours of the different actors in the scenario needs to be modelled through intelligent agents (IAs) and properly mapping policies and doctrines as well as new potential threat behaviours.

In this context, one of the main goals of this research is to couple topologies and characteristics of heterogeneous networks and cyber defence warfare within conceptual models ready to be federated and simulated; this research aims at defining models reproducing objects, attributes and their behaviours and interactions to reproduce heterogeneous networks immersed in operational scenarios and operated by human social networks. For this purpose, the authors have developed a preliminary model, finalised in marine cyber warfare simulator (MCWS) which is the object of the present research.

State of the art 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 analysing the compromise of a deployed tactical network has been proposed by Asman et al. (2011). Homeland security applications were approached in Kotenko (2007), in some work on multi-agent modelling and simulation of cyber-attacks and cyber-defence; 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 US Department of Homeland Security, whose security analysts developed simulation models and tools to analyse the consequences of complex events on critical US infrastructure and resources (Adam et al., 2013); the analysis of ICT infrastructures respect cyber security issues could be addressed even by risk analysis and Monte Carlo simulation using high performance computing (HPC) 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 characterised by dynamic and complex nature (Rumekasten, 1994). Indeed, heterogeneous networks result from an aggregation of different assets, i.e., underwater systems, surface drones, ships, helicopters and even satellites (Eickstedt et al., 2006) being available for connection based on their operative status and boundary conditions; this context is a very sensitive environment in cyber warfare; in this area the conceptual models are representing the characteristics of nodes, connections, and infrastructures of the heterogeneous network (Benjamin et al., 2010)

The use of IAs has been demonstrated to be very effective for reproducing reactive entities and complex systems; the concept of agent-driven simulation where the IAs are directing objects active within the simulation was tested in a wide spectrum of applications (Oren and Ylmaz, 2009). Indeed the capability to reproduce by agent emergent behaviours in complex system is major a benefit of this approach (Thompson and Bossoimaier, 2006).
The IA allows modelling platforms, including humans as well as their interactions (Cornforth et al., 2004; Calfee and Rowe, 2004).

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

3 Interoperable simulation for cyber warfare in heterogeneous 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.

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 analyse 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 finalise new requirements and/or procedures (Guo et al., 2010).

The authors are currently working on researches related to marine heterogeneous networks 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).

Figure 1 Example of a heterogeneous network for an ASW operation involving two AUVs (see online version for colours)

The different conceptual models (representing the characteristics of nodes, connections, infrastructures) 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 synchronised 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).

4 Models and 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 defence topological and procedural aspects regarding complex heterogeneous networks; one crucial part is represented by introducing autonomous and intelligent behaviour over the simulated entities, in this case the simulator was adopting intelligent agents computer.
generated forces (IA-CGF) developed by the simulation team to reproduce threats and behaviours as well as entities’ reactions (Bruzzo et al. 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 combines 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.

The model considers the distinction between the computer information systems representing the cyber infrastructure (CIS infrastructure) and the operational context including the mission and operation type, and all user-related processes that form the operational capability.

Some human behaviours, in fact, could easily compromise a network or its performance owing 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 owing 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 defence 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).

Figure 2  Sensor network case study (see online version for colours)
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 modelling 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 finalise a relevant demonstration within the research timeframe; such finalisation is made possible by the use of simplified meta-models able to approximate the behaviour of the objects. Nevertheless the simulation architecture proposed guarantees the possibility to keep the proposed modelling 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 finalised in MCWS 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 3 MCWS objects (see online version for colours)
The characterisation of the security properties of the nodes, and the links between them, has been conducted through a process of identification of key properties and behaviours; for example, we assume that the integrity factor of one network node affects downstream flows of information; and 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 behaviour 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 modelled and simulated even considering stochastic factors affecting the procedure evolution.

Behaviours 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; the submarine (OPFOR) goal is to move from the 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 is affected by target and sonar platform noise affected by dynamic behaviours as well as by the specific characteristics of the sensor
• active sonar mono-static and multi-static: the model is 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 two AUVs, one destroyer with two helicopters, one 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 anti-submarine warfare (ASW) 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 terms of nodes and connections.

OPFOR have just a submarine armed with torpedo and a cyber-warfare centre transmitting sensitive information through very low communication; in order to simplify the scenario the submarine cyber warfare centre communication is considered very reliable over a wide spectrum of operational modes; obviously the reliability and availability of this connection could be considered subject to all boundary and conditional factors as other connections in the future for more realistic researches.

In this scenario the focus is on three of 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) passes through this cyber resource, the information is transmitted to the submarine, which changes its behaviour 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 reestablished.

The scenario adopted very simple ROEs: 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 will; the ROEs are directed by the IA-CGF (Bruzzone et al., 2011); the authors conducted verification and validation (V&V) 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 modelled 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 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 four 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 the action and the submarine resigns
• 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
Infrastructures protection based on heterogeneous networks

- 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 the authors’ hypotheses as well as other parameters; so the experimental results are characterised as relative values (one with respect to the others) much more than as absolute evaluations.

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

\[
\overline{BFS_{\text{Rate}}}(k) = \frac{\sum_{i=1}^{k} BE_{ES}(i)}{k} \quad (1)
\]

\[
MSP_{BFS_{\text{Rate}}}(k) = \sum_{i=1}^{k} \left[ BE_{ES}(i) - \overline{BFS_{\text{Rate}}}(k) \right]^2 / (k-1) \quad (2)
\]

\[
CF_{BFS_{\text{Rate}}}(k) = \frac{1}{2} \cdot t_{\alpha, k-1} \cdot \sqrt{MSP_{BFS_{\text{Rate}}}(k)} \quad (3)
\]

\[
BE_{ES}(i) = \begin{cases} 0 & \text{if end state of } i^{\text{th}} \text{ run is ship down} \\ 0 & \text{if end state of } i^{\text{th}} \text{ run is sub success} \\ 1 & \text{if end state of } i^{\text{th}} \text{ run is Blue Force success} \\ 1 & \text{if end state of } i^{\text{th}} \text{ run is sub down} \end{cases}
\]

\[
BFS_{\text{Rate}}(k) = \text{Blue Force success rate (BFS rate) after } k \text{ replications}
\]

\[
BE_{ES}(i) = \text{Blue Force in end state of the } i^{\text{th}} \text{ run}
\]

\[
n = \text{total simulation replications changing pseudo random seed}
\]

\[
k = k^{\text{th}} \text{ replication among simulation runs}
\]

\[
MSP_{BFS_{\text{Rate}}}(k) = \text{mean square pure error of BFS rate after } k \text{ replications}
\]

\[
CF_{BFS_{\text{Rate}}}(k) = \text{semi amplitude of the confidence ban of BFS rate after } k \text{ replications}
\]

\[
t_{\alpha, \nu} = r-\text{Student distribution with } \alpha \text{ confidence level and } \nu \text{ degree of freedom.}
\]

MCWS general architecture is designed in order to federate different models into an interoperable simulation environment; therefore in this case it was implemented within a 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 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; the following figures propose only the analysis of the mean square pure error over the different scenario hypotheses (see Figures 5 to 8) and a basic comparison of the overall results (Figure 9).

**Figure 5** MSP and mean BF success in limited scenario without cyber warfare (see online version for colours)
From the analysis the optimal number of replications for each combination of scenario hypotheses emerge: the MSpE and consequently the confidence band results are pretty good even with a limited number of replications;

Figure 9 shows the comparison among the different results changing the scenario hypothesis; the analysis confirms 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 by a collaborative ASW mission “hold at risk/secure friendly manoeuvre area”, conducted via AUVs; therefore the case study proposed represents a relevant mission environment with respect to 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 solutions to complex scenarios; indeed the described approach is open to be extended and applied to more sophisticated contexts.

The use of MCWS allows conducting experimental analysis; by this approach, it is possible to use sensitivity analysis in order to evaluate the most influential parameters, the second and higher 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 behaviours 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 described in this paper confirms the benefits of the proposed approach and the importance of adopting simulation as an investigation aid for cyber warfare within operational frameworks.

References


**Websites**

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