DISTRIBUTED SIMULATION OF ELECTRONIC WARFARE COMMAND AND CONTROL SCENARIOS

Sergio Tortora[(a)], Davide Cannone[(b)], Massimo Giovacchini[(a)], Giuseppe F. Italiano[(b)], Maurizio Naldi[(b)], Andrea Sindico[(a)]

[(a)]Elettronica S.p.A.
[(b)]Dipartimento di Informatica, Sistemi e Produzione, University of Rome "Tor Vergata", Italy

sergio.tortora@elt.it, cannone@disp.uniroma2.it, massimo.giovacchini@elt.it, italiano@disp.uniroma2.it, naldi@disp.uniroma2.it, andrea.sindico@elt.it

ABSTRACT

In this paper we describe the main features of distributed simulation environment we have designed and developed for testing a Command and Control system for distributed Electronic Warfare (EW) Network Centric Operations,

Keywords: Network Centric Warfare, Network Centric Operations, Electronic Warfare, Distributed Simulation

1. INTRODUCTION

The exploitation of networked distributed sensors and actuators is becoming a key factor in military operations. This trend, called network centric warfare or network centric operations (Alberts, Garstka and Stein 2000), allows to have several views of the surrounding environment, which eventually leads to an improved and more precise situation assessment. That's the key to quick and effective decisions.

Different kind of sensors will indeed perceive different characteristics of the same entity. For instance, passive radar detectors, such as Electronic Support Measures (ESM) or Radar Warning Receivers (RWR), are able to detect, measure, and identify radar emissions. Passive communication detectors, such as Communications Electronic Support Measures (CESM), perform the same task on radio signals. Traditional primary radars are capable of detecting the presence of moving targets relying on their radar cross sections. An integrated management of those sensors allows to exploit sensing diversity, spanning several domains, such as space, frequency, and waveform. The inclusion of passive sensors makes the detection task even more effective because of their zero probability of being intercepted by possible opponents.

The exploitation of this wide variety of distributed sensing information is however possible if a proper C4ISR infrastructure is in place. C4ISR is a military acronym standing for *Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance*. The complexity of the functions incorporated in a C4ISR infrastructure makes its definition a challenging task and require a complex chain of definition, design and optimization, and test phases. The very nature of the operations associated to C4ISR makes it impossible to rely on an experimental validation of the strategies envisaged. The test of C4ISR strategies has therefore to be accomplished through simulation.

We have developed a simulator employing the principles of distributed simulation to realize realistic battlefield scenarios and test Command & Control strategies in a C4ISR framework. In this paper we describe the main features of our simulator and report the results of a first test case devoted to analyzing the robustness of routing protocols in a mobile ad-hoc network under cyber attacks.

The paper is organized as follows. In Sections 2 and 3 we describe respectively the simulator as a whole and its module dedicated to the simulation of cyber threats. The test case concerning the robustness of routing protocols is described in Section 4.

2. THE ELT-950 SIMULATOR

In order to test the functionalities of C4ISR systems in a realistic battlefield environment, we have developed a simulator based on the principles of distributed simulation. In this section we review those principles and then describe the structure and characteristics of that simulator, named ELT-950.

Our simulation environment must allow the definition and deployment of network-centric warfare scenarios, with the possibility of automatic generation of inputs. An important requirement for such simulation environment was the capability of scaling well to scenarios having different complexities. Moreover, the possibility to add real systems into the simulation loop was strongly desired.

In order to achieve these requirements we designed a distributed simulation environment consisting of a scenario generator, which continuously updates the status of a scenario in a shared data space implemented through HLA (High Level Architecture), an IEEE standard for distributed simulation (IEEE 2010). The use of HLA allows computer simulations to interact with other computer simulations regardless of the

ISBN 978-88-903724-3-8

computing platforms. The interaction takes place through the Run-Time Infrastructure (RTI), and consists in communicating data and synchronizing actions. The set of computing platforms involved in the simulation is named a federation, and the computing platform themselves (each hosting a simulation entity) are named federates. The federated entities connect to the shared data space through a dedicated bus. The resulting simulation architecture is shown in Figure 1.

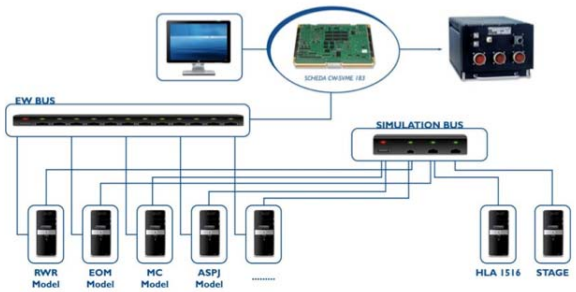

Figure 1: Distributed Simulation Architecture

Through the use of this distributed approach our simulator can boast the following features:

- Wide variety of hosting platforms
- Wide variety of sensors
- Wide variety of actuators
- Wide variety of communications systems
- Location optimization capabilities for sensors
- Integrated situation awareness and assessment
- Full OODA cycle (Observe, Orient, Decide, and Act)

The simulator can include in the battlefield scenario both fixed and moving platforms. The platform may be aircraft, ground vehicles (e.g., tanks or faster tactical vehicles), or ships. Their movement may be simulated by a number of models. In particular the model of our choice is the Reference Point Group Mobility Model (RPGM), which accounts both for movements of groups of vehicles as a whole and for the movements of individual vehicles within the group (Hong, Gerla, Pei and Chiang 1999). Each platform (or each group of platform) is simulated by a different computer in the distributed simulation framework.

Each platform may host a variety of sensors, ranging from radars to ESM systems, Laser Warning Systems, and passive sensors. The platform communicate between them through an ad-hoc network, by employing a number of communications devices (for both data and voice). At the same, we assume platform to host specific devices to accomplish offensive actions against the sensing and the communications capabilities of other platforms. In particular, we may simulate ECM systems, the use of chaff and flares, and attacks on the computing platforms to disrupt the networking capabilities of the platforms (cyber attacks). The simulator includes a meta-model specifically designed to take into account electromagnetic aspects when stating distribution strategies (Sindico, Tortora, Petrelli and Fasano 2010).

The simulator also includes the capability to choose the best location and the best frequency range for each sensor of the suite to maximize the overall surveillance capability. Having different moving passive sensors enables their distribution in space and frequency with the aim of obtaining a wide coverage of detection in both geographic and frequency dimensions. Moving Radars can therefore be distributed, oriented, and tuned, in order to minimize the interferences with ESM. Distribution is important not just to increase the surveilled area but also to allow fine target localization by means of triangulation (Benvenuti and Sindico 2010) or other techniques.

The knowledge gained through the sensors is exploited in the OODA loop, which embodies the Command \& Control capabilities of the C4ISR system. The concept of viewing the combat operations process, even at the strategic level, as a continual loop of four basic activities (Observe, Orient, Decide, and Act) was developed by military strategist and USAF Colonel John Boyd (Osinga 2006). A pictorial representation of that loop is shown in Figure 2.

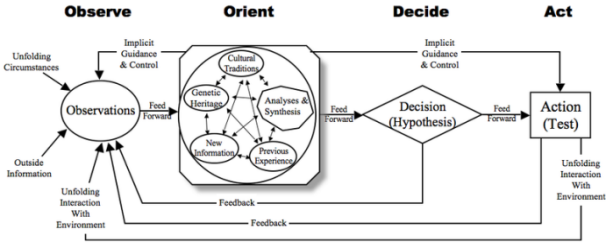

Figure 2: The OODA Loop

In our case the four phases are mapped as follows:

1. Observe → Identify possible threats, their location and evolution over time AND the effect of actions taken at previous rounds of the loop.
2. Orient → Project observations against attack signature databases and learning systems.
3. Decide → Choose the best countermeasure, spanning both the kinetic domain and the electromagnetic/cyber domain.
4. Act → Apply the countermeasure.

3. SIMULATION OF CYBER THREATS

A significant feature of the ELT-950 simulator described in Section 2 is its capability to simulate the occurrence of cyber threats in a mobile environment. The case of mobile platforms moving in a hostile environment and subject to attacks at all levels of the communications protocol stack is a very hard testbed for any simulator. We have therefore considered the simulation of cyber threats as a very first test case for our simulator. In this section we describe the set of cyber threats that the ELT-950 is able to simulate.

ISBN 978-88-903724-3-8

We wish to study the performance of a MANET in a hostile environment, i.e., containing an adversary which aims at downgrading the performance of the network, disturbing the correct functions of the network, or acquiring information about the nodes in the network.

Security issues in MANET have already been discussed in other works (Yang, Luo, Ye, Lu and Zhang 2004; Djenouri, Khelladi and Badache 2005); by studying system vulnerabilities and modeling adversary, a list of cyber attacks have been already consolidated. All of the approaches are related to a discipline called *threat modeling*: it is the process of enumerating and risk-rating malicious agents, their attacks, and those attacks' possible impacts on a system's assets. The benefits of threat modeling are: aiding in prioritizing types of attack to address, helping more effectively in mitigating risk, augmenting assessments with new potential attack vectors, identifying business-logic flaws and other critical vulnerabilities that expose core business assets.

In this section we describe our threat model, that focuses on a generalized view of known cyber attacks to untie the simulation from unnecessary details.

Threats are strictly related to the model of the adversary, so, the first step in threat modeling is to characterize the adversary. In this context our assumptions about the adversary are:

- an adversary can take control of a friendly node, replacing it with a malicious node; this event, in general, happens with a probability different from 100%, and it depends on many factors (e.g., type of intrusion attack, human behavior) but we considered the worst case, where this event happens with a probability of 100%; in this way there is no need to distinguish between internal and external adversaries, and we can assume that an adversary can always get access to the network;
- an adversary can take control of more than one node;
- malicious nodes are mobile;
- malicious nodes can cooperate to attack the system and can communicate on a reserved wireless channel. This means that friendly nodes cannot obtain information about an attack (before the attack itself) and use it to organize a defense;
- friendly nodes cannot detect malicious nodes and organize a defense;
- an adversary cannot deploy malicious nodes on the network before the deployment of friendly nodes. This means that some specific attacks, like Rushing attacks (an attack that acts like a Denial of Service against on-demand ad hoc network routing protocols; it is based on the possibility to forward routing packets before friendly nodes do, to create routes that include malicious nodes; see Hu, Perrig and Johnson 2003), are not achievable;
- malicious nodes are at least as computationally strong as the friendly ones. This means that the former can access as many resources as the latter.

When approaching a simulation, it is necessary to make some assumptions and decide what and how to simulate: indeed, in a simulation, some differences in attacks may not be well perceptible (e.g., Eavesdropping, an attack where the opponent listen passively the wireless channel to sniff packets, versus Traffic Analysis, an attack, in ciphered network, where the opponent try to infer information on the network and its participants by watching characteristics of the traffic (Raymond 2001), and some attacks may not be easily reproducible without adding unnecessary complexity (e.g., Sleep Torture Deprivation, an attack, executed in a network of battery-powered nodes, where the adversary try to exhaust the battery of the node target (Stajano and Anderson 2000) and the necessity to have a power consumption model).

We decided to abstract most from specific attacks, to create a threat model able to represent well the majority of known cyber attacks against a MANET and not to focus on details that cannot be reproduced in the simulation; for example, our threat model does not reckon with security issues in the application layer.

For the purpose of this paper, we define as *fake* a packet sent by a malicious node and as *intercepted* a packet received by a malicious node.

We grouped cyber attacks in four main categories:

- *Denial of Service*: The adversary causes an overloading, an interruption or a disturb in the network such that it begins to misbehave; often this misbehavior represents a downgrade of the performances. The attack can be reproduced by sending to the system more requests that it can handle or by using flaws in protocols used on the system. In the simulator this attack is executed by replacing a friendly node with a malicious one, and forcing the malicious node to send a constant flow of messages towards a target friendly node, at a rate higher than normal communications. All the outgoing packets of the malicious node are tagged as *fake* and all the incoming packets are tagged as *intercepted*. This attack can reproduce a *Distributed Denial of Service* when there is a single target node and multiple malicious nodes.
- *Fabrication*: The attacker fabricates spurious messages, whose nature depends on the attacker's access level to the system, and inserts them in the network; for example, these can be replication of packets that have already traveled on the network, fake signaling messages or packets to promote fake links or fake nodes. In the simulator this attack is

ISBN 978-88-903724-3-8

executed by inserting a malicious node near a friendly one and tagging as *fake* all the packets sent by this node.

- *Interception*: The attacker does not interfere with the network operations and limits itself to eavesdrop packets. The information gained depend on the level of encryption of the system layers. Whenever the adversary cannot obtain any information due to encryption, he can use traffic analysis techniques. By analyzing the messages flows, the attacker can infer information not directly accessible: for example, he can understand that two nodes have different functions by noticing the frequencies of output messages. In the simulator this attack is executed by tagging a friendly node and all the incoming packets as *intercepted*.
- *Impersonation*: The attacker mimics a target node, intercepting its messages and sending packets signed by it. This attack has both the scope to gain sensible information and have an active role in the network; in this way, the malicious node can participate to the distributed operations of the network (e.g., routing) and have the possibility to give fake information. This type of attack is often known as Man in the Middle. In the simulator this attack is executed by replacing a friendly node with a malicious one, and tagging as *fake* all the packets sent and tagging as *intercepted* all the incoming packets.

At last, there is the need to evaluate the impact of a cyber attack towards the analyzed system; other than using metrics related to the performances of the network and of the single nodes, we decided to use as metrics the percentage of the overall *fake* packets received by any friendly node and the percentage of the overall packets *intercepted* by the adversary; these measures are taken at the routing layer.

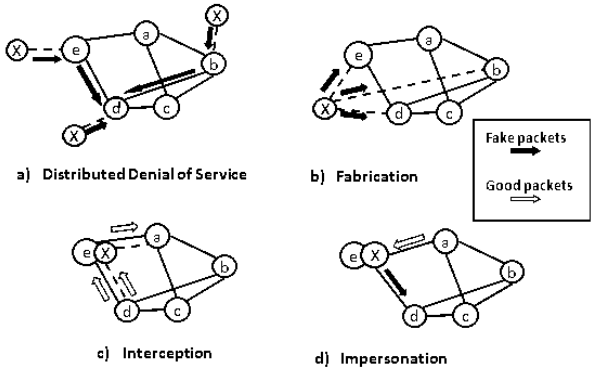

Figure 3: Threat Models

Figure 3 is a graphical representation of the threat model that we have chosen: nodes marked with an X represent malicious nodes, inserted in the network or by replacing a friendly ones; dotted lines represent communication channels with a malicious node.

By modifying properties of these four attacks and combining them, other more specific attacks can be represented in the simulator: for example, in the *Impersonation* attack, when the malicious node does not fabricate any fake packet, this can be a representation of a sinkhole attack (in a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center; see Karlof and Wagner 2003).

4. A TEST CASE: ROBUSTNESS ANALYSIS OF MOBILE ROUTING PROTOCOLS

We have run a first test of the capabilities of our simulator. We have compared the performances of a set of MANET routing protocols in the face of cyber attacks (Cannone, Naldi, Italiano and Brancaleoni 2011). In this section we report a brief overview of the simulation results.

In order to test our simulator we have defined a realistic simulation scenario, considering mobile ad-hoc network operating in a nearly flat geographical area (i.e., there are no relevant obstacles either for movements or signal propagation) extending over 100 square kilometers. Inside the region there are 15 nodes, either fixed (representing base stations) or mobile (representing slow ground vehicles). Every node communicates through bidirectional wireless channels and mounts an omnidirectional antenna. The receiving sensitivity threshold has been set so that any two mobile stations are connected if their distance is lower than 2 kilometers. Any node can generate traffic network towards any other node: the network traffic matrix has random entries, with every flow having a probability of 50% to exist. Every packet source spawns traffic according to an On/Off process with exponential distributions for both On and Off times, and an average rate of 1Mbit/s. The average packet size is 1000 Byte.

As to the routing protocols, in the test case we have considered the following selection of routing protocols (see Akkaya and Younis 2005) for a survey of routing protocols in MANETs):

- Destination-Sequenced Distance-Vector (DSDV);
- Ad-Hoc On-Demand Distance Vector (AODV);
- Dynamic Source Routing (DSR);
- Zone Routing Protocol (ZRP);
- Fisheye State Routing (FSR).

Among them, DSDV and FSR are proactive protocols, where the nodes maintain up-to-date routing information. Instead, AODV and DSR are reactive protocols, setting up routes on demand. Finally, the ZRP is a hybrid protocol, employing the proactive approach for the nodes inside a local area and the reactive one to reach nodes outside of it.

ISBN 978-88-903724-3-8

As to the threat models, we report here the results obtained with a scenario representing an aggressive attack towards the network, composed mostly of malicious nodes performing Denial of Service and Fabrication attacks.

We have considered the following performance parameters:

- Connectivity
- Goodput
- Packet delivery ratio
- Delay
- Percentage of intercepted packets
- Percentage of fake packets

The goodput (expressed in Kbps) is the amount of Kbits of useful data received in time unit, excluding routing information and duplicates. The packet delivery ratio expresses the same quantity, but expressed in packets rather bits. The delay (expressed in milliseconds) is defined as the time between the sending of a message until its complete reception by its recipient. We wish it to be as low as possible, though it will grow with the traffic. The percentage of intercepted packets is the ratio of all packets, tagged as *intercepted*, received by any malicious node, and the number of packets not tagged as *fake*. This metric represents the probability that the attacker gets routing information, breaking the anonymity of the network. A system designer aims at minimizing this metric, especially in scenarios where eavesdropped information can open the door to a more lethal attack; in an encrypted communication layer the system designer must pay attention to internal attackers, who can access network services and intercept packets more easily. The percentage of fake packets is the ratio of all packets, tagged as *fake* and received by any friendly node, and the number of packets received by any friendly node; we exclude packets received by any malicious node. This metric represent the probability that a friendly node receives spoofed or corrupted packets, e.g., with bogus routes or making some weak link more attractive.

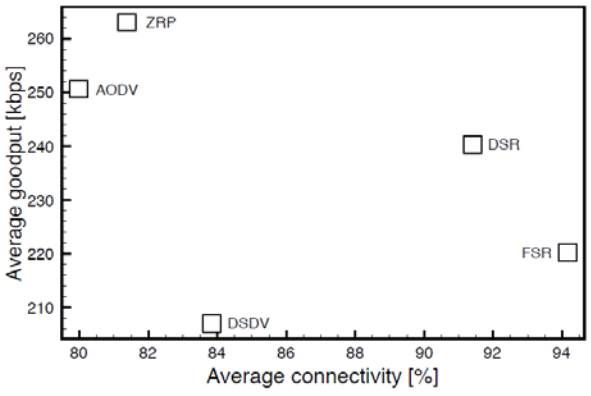

Figure 4: Comparison of Protocols in Sending Data Through

In the first graph, in Figure 4, we show the performance parameters concerning the capability to getting data through. Namely we plot the goodput versus the connectivity. We expect a robust routing protocol to guarantee connectivity and to have as high a goodput as possible. Hence, the best protocols are those positioned on the upper right corner of the graph. Though there is not a clear winner, we see that the reactive protocols perform generally better than the proactive ones.

A second set of results describes again the capability of protocols to get data through (represented by the packet delivery ratio), but compared with the delay experienced by packets. We wish to have a low delay as well as a high delivery ratio. In Figure 5 we show the delay vs. the delivery ratio; in that graph the best performing protocols should appear on the lower right corner. In this case the two proactive routing protocols (FSR and DSDV) are undoubtedly the best.

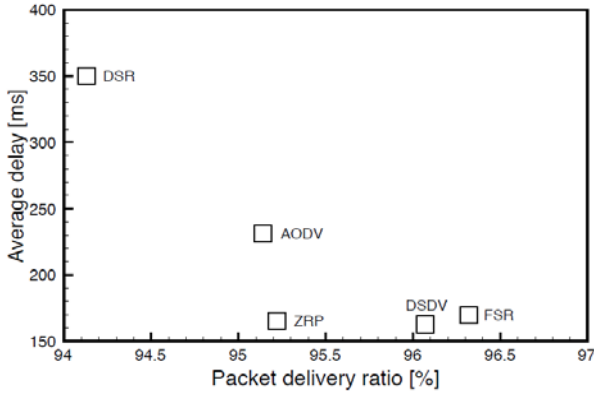

Figure 5: Delay Performances of Protocols

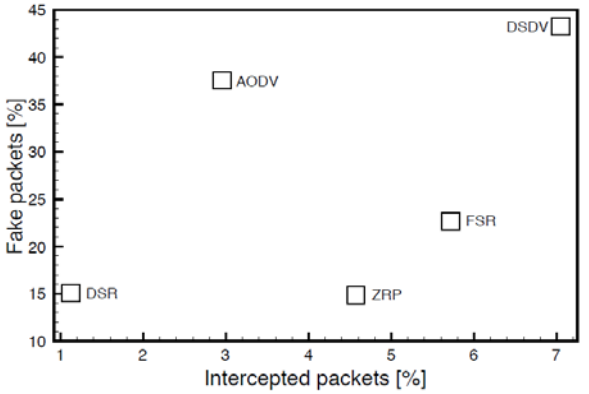

Figure 6: Routing Corruption Performances

Finally, we consider the capability of malicious node to affect the routing mechanisms. In Figure 6 we show the percentage of fake packets versus the percentage of intercepted packets. We wish to have low values for both figures of merit. The best performing protocols are those appearing on the lower left corner. Proactive protocols exhibit a problem, since they send their own routing tables at regular intervals, continuously providing the attacker with up-to-date infos on the network status. On the overall, the reactive DSR is clearly the winner here.

ISBN 978-88-903724-3-8

5. CONCLUSION AND FUTURE WORKS

We have developed a simulator to test Command & Control strategies in distributed electronic warfare command and control scenarios.

The simulator employs the principles of distributed simulation through a HLA architecture, and allows for a wide variety of platforms, sensing and communications devices, as well for attacks over the whole protocol stack.

We have run a first test case for the simulator to evaluate the robustness of routing protocols to cyber attacks. For a scenario where the majority of attacks are of the Denial of Service and Fabrication type, we have shown that reactive protocols appear as the most robust, though they are affected by larger delays.

What presented is the first result of an ongoing work. The next steps encompass a classification of communication packets with respect to the electronic warfare function to which they relate (i.e. passive search, emitter tracking, jamming, etc.). This is important to also evaluate the consequences in the EW domain that could derive from an attack to the network. Another important feature we are about to introduce is the capability of evaluating the best assignment of platforms position and functionalities (i.e. Radar search, passive search, countermeasures, etc.) in order to maximize the surveilled area within a range of frequencies chosen by the operator.

REFERENCES

Alberts, D.S., Garstka, J.J., Stein, F., 2000. *Network Centric Warfare: Developing and Leveraging Information Superiority (2nd Edition)*. CCRP Press.

Akkaya, K., Younis, M., 2005. A survey on routing protocols for wireless sensor networks. *Ad hoc networks*, 3 (3), 325-349.

Benvenuti, D., Sindico, A., 2010. Design and simulation of a distributed sensor network for passive emitter tracking and coast surveillance. *Proceedings of the International Waterside Security Conference*, pp. 1-5. November 3-5. Carrara (Italy).

Cannone, D, Naldi, M., Italiano, G.F., Brancaleoni, A., 2011. A simulator of a mobile ad-hoc network in a hostile environment. *Proceedings of the 1st International Conference on Simulation and Modeling Methodologies, Technologies, and Applications, Simultech*. July 29-31, Noordwijkerhout (Netherlands).

Djenouri, D., Khelladi, L., Badache, A.N., 2005. A survey of security issues in mobile ad hoc and sensor networks. *Communications Surveys & Tutorials, IEEE*, 7 (4), 2-28.

Hong, X., Gerla, M., Pei, G., Chiang, C.C., 1999. A group mobility model for ad hoc wireless networks. *Proceedings of the 2nd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, pp. 53-60. August 20-20. Seattle (Washington, USA).

Hu, Y.C., Perrig, A., Johnson, D.B., 2003. Rushing attacks and defense in wireless ad hoc network routing protocols. *Proceedings of the 2nd ACM workshop on Wireless security*, pp. 30-40. September 19-19, San Diego (California, USA).

IEEE, 2010. IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)-- Framework and Rules. *IEEE Std 1516-2010 (Revision of IEEE Std 1516-2000).* August 18, 1-38.

Karlof, C., Wagner, D., 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, 1 (2-3), 293-315.

Osinga, F., 2006. *Science, strategy and war: the strategic theory of John Boyd*. USA: Routledge.

Raymond, J.F., 2001. Traffic analysis: Protocols, attacks, design issues, and open problems. *Proceedings of International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability*, pp. 10-29. Berkeley (California, USA).

Sindico, A., Tortora, S., Petrelli, A.C., Fasano, M.V., 2010. *Proceedings of the 2nd International Workshop on Cognitive Information Processing*, pp. 23-28. June 14-16. Elba (Italy).

Stajano, F., Anderson, R., 2000. The resurrecting duckling: Security issues for ad-hoc wireless networks. *Proceedings of Security Protocols Workshop*, pp. 172-182. April 3-5. Cambridge (UK).

Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L., 2004. Security in mobile ad hoc networks: challenges and solutions. *Wireless Communications, IEEE,* 11 (1), 38-47.

ISBN 978-88-903724-3-8