A SIMULATION STUDY OF C4I COMMUNICATIONS NETWORK UNDER CYBER ATTACKS

Agatino Mursia[(a)], Lucio Ganga[(a)],
Alessandro Leonardi[(b)], Giacomo Morabito[(b)], Corrado Rametta[(b)], Lloyd Wihl[(c)]

[(a)] Selex Elsag Spa, Italy
[(b)] Dipartimento di Ingegneria Elettrica, Elettronica ed Informatica, University of Catania, Italy
[(c)] Scalable Network Technologies, Inc. USA

[(a)] Name.Surname@selex-comms.com, [(b)]Name.Surname@dieei.unict.it, [(c)]lwihl@scalable-networks.com

ABSTRACT

The use of wireless communications in today's tactical networks is a necessity but at the same time increases the vulnerability to cyber attacks. It is essential to consider the effects of these attacks during network design and operation. Network simulation software, which employs models of real tactical radios, and hardware in the loop functionalities, can be very useful to evaluate the effects of such attacks on the system performance. In this paper, we present the results of our study aimed at investigating the behavior of wireless communication networks under some common cyber attacks and we also consider the effect of some countermeasures in order to minimize the effects caused by the attacks.

Keywords: simulations, EXata/Cyber, human in the loop, performance, cyber warfare, networks

1. INTRODUCTION

The use of wireless communications in tactical scenarios has gained a primary role in the modern approaches of patrol and fight (Maseng and Nissen 2008).

The units involved in tactical warfighting are more and more often equipped with electronic devices able to exchange, through a data flow (continuous or burst), sensitive contents with other units located in the same geographical area and/or with higher hierarchical levels. The adoption of these new technologies allows a strong interaction among the different components involved in the operation and improves the coordination and efficacy of the action in the area of interest.

However, the use of these technologies implies, necessarily, an increase of the risks coming from cyber attacks towards the network and the supported data flows.

Consequently, it becomes mandatory, during the design of network architectures and the selection of proper communication protocols, to take into account the above issues and dispose the required procedures to counteract them (Lipson 2002, Di Pietro 2002).

One of the most efficient ways to achieve the above objectives is the use of simulation software. This software can be employed both in the design phase of networks and equipment, and in the planning of operations. The flexibility, modularity and performance prediction make simulation software essential to validate the architectural choices related to the networks and equipment to be employed in the different scenarios.

The goal of this paper is to discuss the results of our study aimed at investigating, through different simulation scenarios, the behavior of wireless communication networks under some particular cyber attacks. The scenarios under investigation are characterized by teams and/or mobile units operating in a specified area and using communication facilities having Mobile Ad hoc NETworks (MANET) capabilities. The considered scenarios include models representing the operational functions of some communication radio devices working in extra-urban areas.

These models are derived from the real tactical radio devices and integrate software models that implement protocols related to levels 1, 2 and 3 of the ISO/OSI protocol stack, created "ad hoc" to counteract and/or minimize the damage caused by the cyber attacks.

Simulation environments are deployed by using specialized software simulators. In this paper we use EXata/Cyber®, (Scalable Network Technologies 2011), in order to simulate the communication network architecture, the radio devices employed, and the cyber attacks and defenses.

Moreover, EXata/Cyber® provides hardware-in-the-loop (HITL) functionalities which we exploit to connect systems running real applications in order to obtain a more realistic behavior of the traffic sources.

In particular, we focus on command, control, communications, computers, and (military) intelligence applications (C4I) which play a key role in tactical and

ISBN 978-88-903724-3-8

military missions. Data flows generated by hardware-in-the-loop devices go across the simulated network in the same way they cross the real one, allowing to estimate the effects of cyber attacks on the effectiveness and reliability of the data transfer among sources and destinations, (Shen 2009).

Moreover, we describe and provide the performance of some countermeasures (network architectures, network protocols, etc.) with the aim of reducing the effects of the cyber attacks taken into account in our study.

The rest of this paper is organized as follows. In Section 2 we will describe the system model. In Section 3 we will describe the elements which compose the system architecture. In Section 4 we will describe the considered scenarios and in Section 5 we will show the results obtained. Finally, in Section 6 we will draw our conclusions.

2. SYSTEM MODEL

We consider a MANET consisting of *N* mobile wireless nodes deployed in an extra-urban area. In order to protect communications, all nodes use the following security procedures:

- MAC layer protection: where access to the MAC layer is protected by specific mechanism (i.e., crypting or frequency hopping).
- Network/Application layer encryption: this ensures that adversary cannot read messages exchanged at the application layer.

Accordingly, it is difficult for the adversaries to attack the network, unless they have gained control over a certain number, say *M* (with *M>0*) nodes.

In fact, if this is the case, the adversaries can perform different types of attacks depending on the protocol layers that they are able to modify.

In particular,

- if they can introduce modifications at the physical/link layer, they can perform jamming attacks. In particular, a malicious node transmits continuously over a channel with sufficiently high power such that all other nodes in the vicinity are unable to send or receive any other signals. This creates a reduction in the network throughput and a decrease in the battery duration.
- If they can introduce modifications at the network layer, they can perform routing attacks. In this case the adversaries create inconsistencies in the routing tables or try to break end-to-end paths between the pairs source/destination.
- If they can introduce modifications at the application layer, they can perform Denial-of-Service (DoS). In this case the nodes controlled by the adversaries generate a large number of service requests for a certain number of nodes so as to cause interruption of the service they provide (note that in ad hoc networks a service provided by all nodes is relaying traffic).

In this paper we study the impact of such attacks on the network performance. More specifically we consider the impact of the knowledge of the adversaries about the technical solutions utilized by the network on the attack effectiveness. For example, if the adversaries know the routing protocol utilized by the network, then they can attack the node that is the most critical for the current topology. If the adversaries know the characteristics of the MAC protocol utilized, then they can perform a more effective jamming attack.

3. SYSTEM ARCHITECTURE

In order to study the impact of the previously described cyber attacks on the system performance, we have considered a testbed which uses both simulated and real devices.

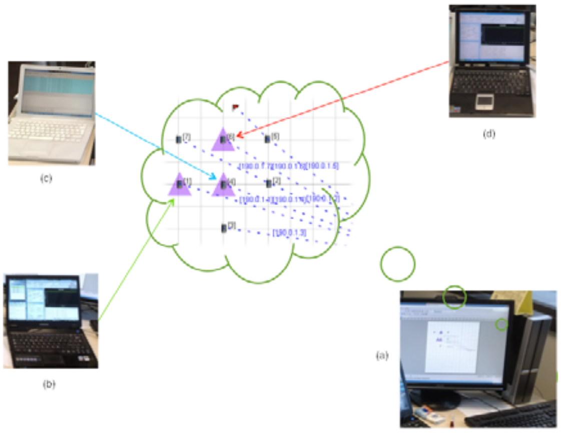

Figure 1 - System Architecture

The system architecture, shown in Figure 1, is composed of the following parts:

3.1. Emulation platform

The emulation platform is realized using a computer desktop running Windows OS and the EXata/Cyber® software suite (Figure 1.(a)). In the emulation platform we can choose the number of nodes, *N*, the physical parameters such as the radio type, frequency, antennas type, etc., the MAC layer, the routing protocol if needed, and the nodes' movement pattern.

3.2. Traffic source

The traffic source, which represents the C4I communication sender, has be modeled in two ways, according to the scenario of interest. The first is using an EXata/Cyber® virtual node, the second is using a notebook running Windows OS together with the *connection manager* tool, and the *iperf* tool running in client mode (Figure 1.(b)). The iperf tool emulates UDP or TCP traffic sent by the node. This real notebook is then mapped inside the EXata/Cyber® emulator as a mobile or fixed node.

3.3. Traffic destination

The traffic destination can be realized in two ways, as a synthetic or emulated node, similarly to the traffic source. Concerning the second way, the *iperf* tool is

ISBN 978-88-903724-3-8

used in server mode (Figure 1.(c)) and this real notebook will then be mapped inside EXata/Cyber® to a mobile or fixed virtual node.

3.4. Malicious node

The malicious node can be realized either as a virtual node inside EXata/Cyber® or as a notebook running Windows OS with the EXata Connection Manager tool which will be mapped to a virtual node in EXata/Cyber® (Figure 1.(d)). The choice of configuration will be related to the scenario of interest.

4. SCENARIOS

We have investigated three different network scenarios. All three scenarios use radio models, with a channel capacity of 2 Mbit/s and a radio range of 250 m. In scenario 1, we have simulated a DoS attack and we have considered the effect of a jammer node against the node which performs DoS. In scenario 2, we have simulated the use of directional antennas in order to reduce the 'eavesdropping' effect. Finally, in scenario 3, we have compared the performance of some common wireless ad hoc routing protocols when there are some jammer nodes in the area.

4.1. Scenario 1 - DoS attack

This scenario is characterized by N = 7. The location of the nodes in the field of interest is shown in Figure 2. We consider a malicious node (M = 1), identified in Figure 2 as node 6, performing a DoS attack against node 4 which represents the traffic destination of a communication initiated by node 1. Both the data communication (node 1 - node 4) and the DoS attack are realized using the *iperf* tool, (Iperf, 2001), and are characterized by the following parameters: size of UDP packets equal to 512 bytes, bit rate equal to 2 Mbit/s, duration 300 s. The DoS attack lasts for 240 s starting from time t = 60 s. The considered countermeasure is realized by identifying the source of the DoS, i.e., node 6, and using a jamming attack against this node. The node which realizes this countermeasure is node 5 which is a virtual node simulated inside EXata/Cyber®. In particular, node 5 moves in the neighborhood of node 6 and once arrived inside its coverage area it starts the jamming attack. The jamming attack is implemented through the HITL command interface of Exata/Cyber®. The jamming attack consists in transmitting continuously over a channel with sufficiently high power, such that all other node in the vicinity of the jammer and communicating on the same channel will find the channel busy, and therefore, will not be able to transmit or receive any other communication.

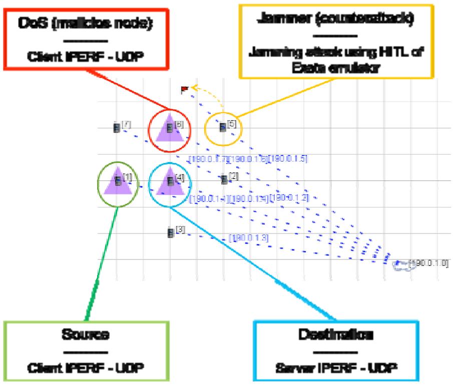

Figure 2 - Scenario 1

4.2. Scenario 2 - Eavesdropping

This scenario is characterized by N = 16. The location of the nodes in the field of interest is shown in Figure 3. We consider a malicious node (M = 1), identified in Figure 3 as node 16, which is able to *sniff* the data traffic flowing in the network. We consider data communication which is both encrypted and unencrypted. In the first case, the malicious node can only locate the nodes involved in the communication; in the second case, the malicious node can also decode the data packets. The *sniffing* procedure is performed using the "eavesdropping" capability implemented in EXata/Cyber® which is modeled as the node's MAC layer operating in promiscuous mode, and enabled to promiscuously listen to nearby wireless communications. Data communication is realized through four CBR data flows, and is characterized by the following parameters: size of UDP packets equal to 512 bytes, bit rate equal to 41 kbit/s, duration 60 s. The eavesdropping attack starts at the beginning of the simulation (time t = 0 s). The malicious node moves inside the simulation field along an established path, as shown in Figure 3. Because it is not possible to identify the eavesdropper node (which is implemented as a passive node) and consequently reducing its functionality (for example using jamming), the considered countermeasure is to use directional antennas both in the source/destination nodes and relayers involved in the communication. The directional antennas are modeled in EXata/Cyber® using the *switched-beam antenna* which is a special type of patterned antenna having different gains in different directions. The switched-beam antenna utilizes multiple antenna patterns and switches the pattern according to the direction of arrival or transmission.

ISBN 978-88-903724-3-8

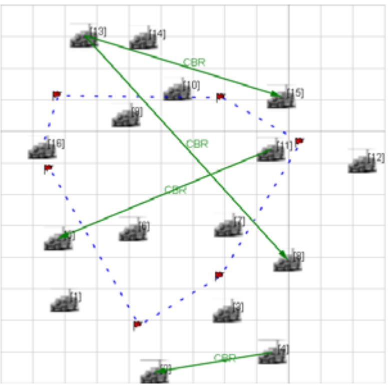

Figure 3 - Scenario 2

4.3. Scenario 3

This scenario is characterized by N = 50 nodes. The location of the nodes in the field of interest is shown in Figure 4. In particular, they are located in a square grid pattern (distance between nodes equal to 200 m) in order to have a better knowledge of the routing protocol's capability to change the path when the attack starts. We consider two malicious nodes (M= 2) moving inside the area using a random waypoint mobility model with the following parameters: range of velocity: 0 - 108 km/h and pause time equal to 20 s. The malicious nodes perform a jamming attack against all the relayer nodes in their neighborhood. The coverage range of the jammer is equal to 125 m. The jamming attack is modeled using the EXata/Cyber® capabilities as in scenario 1. Data communication is realized through five CBR data flows, and is characterized by the following parameters: size of UDP packets equal to 512 bytes, bit rate equal to 102 kbit/s, duration 300 s. The jamming attack starts at the beginning of the simulation (time t = 0 s). The routing protocols considered are: AODV (Perkins 1999, Johnson 1994) and ANODR (Kong 2003). In Section 5.3, we will compare the performance of the routing protocols in terms of robustness to find an alternative path.

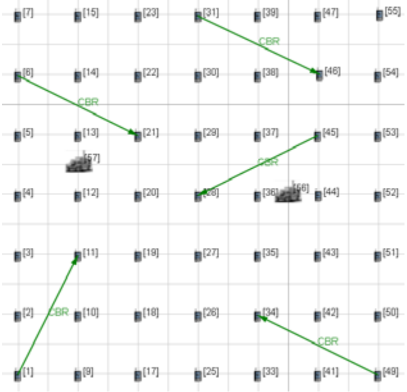

Figure 4 - Scenario 3

5. RESULTS

In this section we describe the impact of the considered attacks and the benefits of the chosen countermeasures on the system performance.

5.1. Results of Scenario 1

In scenario 1 we evaluated both the throughput and the jitter values related to node 4, because these metrics show both the impact of the attack and the efficacy of the countermeasure. Looking at Figure 5 it is possible to note that from t = 0 s to t = 60 s, the number of packets received from node 1 and the related jitter are almost constant. In particular, the value of the received bits corresponds to the maximum value achievable in the communication. Once the DoS attack starts, at time t = 60 s, we observe that the value of throughput becomes unstable, fluctuating in a wide range and sometime reaching the zero value. The value of the jitter increases accordingly. This trend lasts until t = 140 s, which is the time needed for the node 5 to identify the malicious node 6 and starting a jamming attack against it. As a result, node 6 is inhibited to transmit data packets to node 4, and the throughput value again reaches the maximum value such as at the beginning of the test.

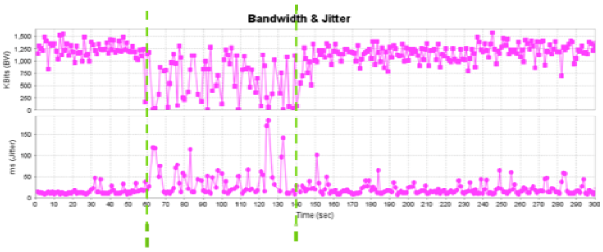

Figure 5 - Results of Scenario 1

5.2. Results of Scenario 2

In scenario 2 we evaluated the differences in the number of packets *sniffed* by node 16 (i.e., packets flowing in the network and received by node 16), when using omnidirectional antennas, and when using directional ones. From Table 1, we note that, as expected, when using the directional antennas, the number of data packets sniffed by the malicious node is reduced when compared to the case when the nodes use omnidirectional ones. This is because, with directional antennas, it is more difficult for the malicious node to be in the radio coverage of the nodes involved in the communication.

	With omnidirectional antennas	With directional antennas
Number of sniffed packets	1476	902
Percentage of sniffed packets over the total number of packets flowing in the network	30 %	18 %

Table 1 - Results of Scenario 2

5.3. Results of Scenario 3

In this scenario, we evaluated the performance in terms of throughput (percentage of received packets), delay and jitter, of the following routing protocols: AODV and ANODR. During the simulation runs we observed that the AODV protocol is the most reactive one. In fact, when the jamming attack is active, the AODV

ISBN 978-88-903724-3-8

protocol succeeds almost always to find an alternative path towards the destination. This is the reason for the higher percentage of received packets when compared with ANODR. However, if we look at the values of delay and jitter, we note that ANODR shows better performance. This is due to the fact that the values of delay and jitter for the ANODR are calculated considering only the packets which reach the destination when the jammer is inactive, and consequently these packets show less delay because they follow the route with the minimum number of hops.

	AODV	ANODR
Percentage of received packets	88.53 %	67 %
End-to-end delay [s]	0.504	0.107
Jitter [s]	0.012	0.003

Table 2 - Results of Scenario 3

6. CONCLUSIONS

In this paper we used a high fidelity software emulation of networks that includes cyber warfare models, EXata/Cyber, to evaluate the effects of some common cyber attacks on the effectiveness and reliability of the data transfer between sources and destinations in a wireless MANET. We also investigated the effect of some countermeasures on the system performance. Results from the software emulation were in accordance with expectations.

ACKNOWLEDGMENTS

We would like to thank Riccardo Rovelli and Amanda Zanotti of Antycip Simulation for providing the EXata/Cyber® emulation software.

REFERENCES

Di Pietro, R., Me, G., 2002. Military secure communications over public cellular network infrastructure. *Proceedings of MILCOM 2002*.

Iperf, 2001. Available from: http://sourceforge.net/projects/iperf/

Johnson D. B., 1994. Routing in Ad Hoc Networks of Mobile Hosts. *Proceedings of the Workshop on Mobile Computing Systems and Applications*.

Lipson, H. F., 2002. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Techical Report. Available from: http://www.cert.org/archive/pdf/02sr009.pdf

MAK, 2011. Available from: http://www.mak.com

Maseng T., Nissen, C.A., 2008. Network centric military communications. *IEEE Communications Magazine,* 46(11), 77-78.

Perkins C. E., Royer E. M., 1999, Ad-hoc on demand distance vector routing. *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99).*

Scalable Network Technologies, 2011. Available from: http://www.scalable-networks. com

Shen, J., Gan, Z., Gang, C., 2009. The Study of Military Simulative Training Based on "Network in the Loop". *Proceedings of Computer Network and Multimedia Technology.*

Kong J., Hong X., 2003. ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks. *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing (MobiHoc '03).*

Wihl L., Varshney M., Kong J., 2010. Introducing a Cyber Warfare Communications Effects Model to Synthetic Environments. *Proceedings of the Inter-service / Industry Training, Simulation and Education (I/ITSEC) Conference 2010.*

Bruzzone A.G., Cantice G., Morabito G., Mursia A., Sebastiani M., Tremori A. (2009) "CGF for NATO NEC C2 Maturity Model (N2C2M2) Evaluation", *Proceedings of I/ITSEC2009, Orlando, November 30-December 4*

Tremori A. (2010) "Research activities about usage of Intelligent Agents and Computer Generated Forces (IA-CGF) for Asymmetric and Non Conventional Operations", *Invited Speech, NATO CAX Forum2010, Munich Germany, August 30/September 2*

Bruzzone A.G. (2010) "CGF & Data Fusion for Simulating Harbor Protection & Asymmetric Marine Scenarios", *Proceedings of SIM&SEA2010, La Spezia, June 8*

Alessandro Leonardi received the Laurea degree in Electrical Engineering and the Ph.D. degree in Computer and Telecommunications Engineering from the University of Catania, Catania (Italy), in 2002 and 2007, respectively.

From September 2005 to February 2006, he was a visiting student with the RNG, Rice University, Houston, TX, under the guidance of Prof. Edward Knightly. Currently, he is a Post-Doctoral Researcher with the DIEEI, University of Catania. His research interests include design and performance evaluation of telecommunication protocols and algorithms, in particular in the area of wireless communications and networking.

Giacomo Morabito was born in Messina, Sicily (Italy) on March 16, 1972. He received the Laurea degree in Electrical Engineering and the PhD in Electrical, Computer and Telecommunications Engineering from the Istituto di Informatica e Telecomunicazioni, University of Catania , Catania (Italy), in 1996 and 2000, respectively. From November 1999 to April 2001, he was with the Broadband and Wireless Networking Laboratory of the Georgia Institute of Technology as a Research Engineer. Since April 2001 he is with the Dipartimento di Ingegneria Informatica e delle Telecomunicazioni of the University of Catania where he is currently Associate Professor. His research interests focus on analysis and solutions for wireless networks.

Corrado Rametta received the Laurea degree in Electronics Engineering from the University of Catania, Italy, in 2008. His final Thesis was on "Study and Evaluation of an Adaptive Technique for Collisions Control in IEEE 802.11 Networks".
He is currently a Ph.D. student with the DIEEI of the University of Catania under the guidance of Prof. Sergio Palazzo. His research interests include: wireless mesh, ad hoc and sensor networks, performance analysis of communication networks.

Lucio Ganga received the Laurea degree in Telecommunications Engineering from the University of Catania, Italy, in 2008. From September 2008 to April 2009 he has done a period of stage at Selex Communications (a Finmeccanica Company). Currently he is a System Engineer at Selex Elsag, and his skill are Network Simulations and interoperability between different Simulation tools through HLA Protocol.

Lloyd Wihl joined Scalable Network Technologies (SNT) in January 2006, where he is Senior Application Engineer, providing worldwide pre-sales support for potential clients, developing system prototypes and technology interfaces, guiding future product development, providing guidance for customer model development, training customers, and managing customer engineering service contracts.
He has over 29 years of experience in the Modeling, Simulation and Training industry. His experience prior to SNT includes 24 years at CAE, where he developed system architectures for military simulation and training, and led multi-million dollar projects in the areas of synthetic military environments, network-centric systems, distributed mission training, air traffic management, space systems, visual systems, and flight simulation.

Agatino Mursia, currently with SELEX Elsag Spa as Head of the Modeling and Simulation (M&S) team of the BU Coomunication for Defence Systems, graduated in Electronics Engineering at the University of Padua in 1989. Since then he has been working in the industry, first with Selenia Spazio Spa, Marconi Italia and then Marconi Communications USA as responsible for the development (Hw and Sw) of communication and networking equipments.
Back to Italy, in 2003 he was appointed as responsible of M&S activities with the role of exploring and promoting the use of M&S as a competitive advantage of products/solutions. He has promoted the use of COTS tools and international simulation standards for the Modeling and Simulation of communications and networking effects into the definition and validation of complex net-centric architectures.
He is also the chairman of the Finmeccanica MindSh@re community SET2 dedicated to simulation that includes most of the Group companies.

ISBN 978-88-903724-3-8