Int. J. Communications, Network and System Sciences, 2015, 8, 533-542
Published Online December 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.813048

Scientific Research Publishing

Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite

Şadan Cambazoglu[1], Arif Sari[2]

[1]Department of Management Information Systems, European University of Lefke, Lefke, Cyprus
[2]Department of Management Information Systems, Girne American University, Kyrenia, Cyprus
Email: sdn1991@gmail.com, arifsari@gau.edu.tr

Received 3 July 2015; accepted 27 December 2015; published 30 December 2015

Abstract

Jamming attack is quite serious threat for Mobile networks that collapses all necessary communication infrastructure. Since mobile nodes in Mobile Ad Hoc Networks (MANET) communicate in a multi-hop mode, there is always a possibility for an intruder to launch a jamming attack in order to intercept communication among communication nodes. In this study, a network simulation has been carried out in order to explore and evaluate the possible impacts of jamming attack on MACAW protocol. Ad-hoc network modelling is used to provide communication infrastructure among mobile nodes in order to modelling the simulation scenarios. In simulation model, these nodes have used AODV routing protocol which is designed for MANET while second scenario contains simulated MACAW node models for comparison. On the other hand, this paper is the first study that addresses performance evaluation of MACAW protocol under a constant Jamming Attack. The performance of MACAW protocol is simulated through OPNET Modeler 14.5 software.

Keywords

OPNET, Simulation, MACAW, Mobile Ad-Hoc Networks, Collision, Jamming, AODV

1. Introduction

Wireless networks take important place in the world of communication. Today a great number of people such as businessmen, managers, students and employees can easily access to the internet or to the corporate networks through wireless connections. Although wireless technologies expand the limits of communication area, they are exposed to some problems due to their nature. These problems violate quality of wireless communication.

How to cite this paper: Cambazoglu, Ş. and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. *Int. J. Communications, Network and System Sciences*, **8**, 533-542.
http://dx.doi.org/10.4236/ijcns.2015.813048

Collision, one of these problems occurs when two nodes in the same network, attempt to transmit data at the exact same time [1]-[4]. Corresponding problem results in loss of quality in communication. Especially in mobile wireless networks collision avoidance issue becomes more difficult due to transmission environment. Up to now, considerable solutions addressing to this problem have been proposed in variety of researches.

MACAW, one of these solutions provides effective collision avoidance mechanisms. MACAW protocol is generally used in mobile wireless networks [4]-[6].

On the other hand, security attacks which are another reason for collision occurrence, result in loss of quality in communication as well. In this study, a network simulation has been carried out in order to evaluate performance of MACAW protocol. During this simulation, MACAW protocol has been exposed to a constant Jamming Attack which results high collision occurrence rate in the network. The entire network mechanisms are simulated through OPNET Modeler 14.5 simulation software which is widely used in the network industry to estimate behaviors of network component in a virtual environment. The importance of this study is the first simulation case that addresses performance evaluation of MACAW protocol under a Jamming Attack.

2. Collision in Mobile Wireless Networks

In computer networks, there are many nodes and they have to transmit data packages over the same carrier. This carrier can be an optic cable in wired networks while it is a frequency in wireless networks. Owing to this networking principle, if two nodes in the same network attempt to send data packages to the communication line at the exact same time, a collision occurs. Collisions are important problems for networks because they violate data transmission and results in loss of information. When any collision occurs in the network, the communication stops; ultimately, data packages are dropped. Collisions always results in less throughput of the network, high network load, high delay and high data drop rate [7]-[9].

2.1. Collision Avoidance Protocol in Mobile Wireless Networks

As mentioned previously, owing to collisions, network nodes face with loss of packet integrity. That means a proper communication cannot be established in the network. In seven layer OSI model [10]-[12], Media Access Control (MAC) layer is responsible for avoidance of package collision. MAC sub layer performs this task through avoidance protocols. These protocols play a critical role in preventing data collision; they aim to rule situations out which multiple nodes access to the network at the exact same time and to provide packet transmission to any node without any collision. There are some protocols that mostly used and are developed to prevent collisions in the networks such as ALOHA, CSMA, MACA and MACAW.

MACAW Protocol

Multiple Access with Collision Avoidance for Wireless (MACAW) is a widely used MAC sub layer protocol. MACAW is useful for mobile ad-hoc networks. It contains new collision avoidance mechanisms. By these mechanisms data transmission is completed in five steps. These five steps are Request-to-Send (RTS), Clear-to-Send (CTS), Data Sending (DS), data packages and Acknowledgement (ACK). RTS is a message, sent from data sender node to receiver node, notifies that a node attempts to transmit data to another node. CTS message is a respond for transmission request. If receiver node available for transmission then sends a CTS message. DS frame informs receiver node about the size of data package. After that, data transmission starts. When it completes properly, receiver node sends an ACK message to sender node. ACK notifies that data transmission completed successfully [13]-[16].

3. Network Simulation

In computer networking field, testing a complete network's behaviors in a real environment is a quite costly process. In this case network simulation techniques provide an opportunity to test network equipment such as routers, servers and cables in an inexpensive way. Besides that, network protocols, networks services and other network features can be tested to see behaviors of nodes. Network simulation actions are performed by network simulators in a virtual environment. A network simulator is a software application that estimates behaviors of nodes, equipment and protocols of a modelled network. Simulators typically support commonly used networking technologies such as Wi-Max, WLAN, and ZigBee. Most of these simulators have a Graphical User Inter-

face (GUI). As well as GUI simulators, Command Line Interface (CLI) simulators are also available. Some network simulation software are open source while some are proprietary software. Commonly used simulators are GNS3, ns, OPNET, NetSim, OMNeT++ [17] [18].

3.1. Simulated Node Models

In this simulation experiment while evaluating collision effects on network, mobile nodes have been used. These mobile nodes create an ad-hoc network among them. In OPNET simulator these types of nodes are called as "manet_station_adv". While simulating scenario, 50 nodes were used.

3.2. Simulation Model and Experiment Environment

While performing simulation scenarios, OPNET Modeler 14.5 has been used. In this simulation, 2 different scenarios are designed. The simulation was performed in a 1000 × 1000 meters campus area with 50 mobile nodes. These nodes share the common parameter attributes. In **Table 1**, all global simulation parameters are shown in detail.

In this simulation model, MACAW and AODV protocols are used. The performance evaluation and contents of the protocol is exposed by the researchers in the literature before [19] [20]. MACAW as mentioned before, is a powerful collision avoidance protocol and used in this simulation model for its specific purpose. On the other hand Ad hoc On-Demand Distance Vector (AODV) [2] is a routing protocol that is used in mobile ad-hoc networks while nodes determining their destination paths for data transmission. Simulation has been carried out for 1 hour in a 1000 × 1000 meters area, Mobility Model status was stated as Simple Random Waypoint with constant speed of 10 meter/seconds. Network Throughput, Network Load and Delay parameters are taken as Performance Parameters. Data Rate was set as 11 Mbps which is maximum data rate for IEEE 802.11 b. Trajectory

Table 1. Simulation scenario parameters.

Parameters	Attributes
Protocols	MACAW-AODV
Simulation Time	1 Hour
Simulation Area	1000 × 1000 (meters)
Mobility Model	Simple Random Waypoint
Mobility m/s	1/10
Performance Parameters	Throughput, Network Load, Delay, Drop Rate
Transmit Power (W)	0.005
RTS Threshold (bytes)	1024
Data Rate (Mbps)	11 Mbps
Pkt. Reception power Threshold	−95 dbm
Buffer Size	1024,000
Pkt. Size (bits)	2000
Pkt. Interarrival time (seconds)	0.03
Trajectory	VECTOR
Start time (seconds)	10
End Time	End of Simulation
No of Seeds	40,000

was set as Vector which means mobile nodes change their location unsymmetrically. Finally, Seed value which is number of network events performed in 1 second, was set as 40,000. The successful simulation scenarios have been conducted on simulated different contention-based or contention-less protocols through OPNET in the literature [19] [20]. So it is quite reliable to conduct this simulation scenario through OPNET simulation package.

3.2.1. Simulation Scenario 1

In the first scenario, there are 50 mobile nodes that have an ad-hoc network among them. They move at a constant speed of 10 meters per second. **Figure 1** below illustrates these nodes distributed randomly in a 1000 × 1000 meters area.

In this scenario illustrated, Application profile, Profile configuration and Mobility configuration are defined to meet network requirements specified in **Table 1**. Network model has two scenarios. In first scenario, nodes communicate with each other in a proper way. There is no malicious node and no security attack. One of these nodes acts as an Access Point at the same time. OPNET simulator has evaluated this scenario for 1 hour. Simulation results were measured and evaluated according to network performance metrics. The main purpose for this scenario is to determine status of network under normal conditions. This scenario will be useful while comparing effects of collisions and security attacks to network performance.

3.2.2. Simulation Scenario 2

In this scenario again 50 mobile nodes have been used. Unlike Scenario 1, here also 3 mobile jammer nodes have been used. Scenario 2 is shown on the **Figure 2**.

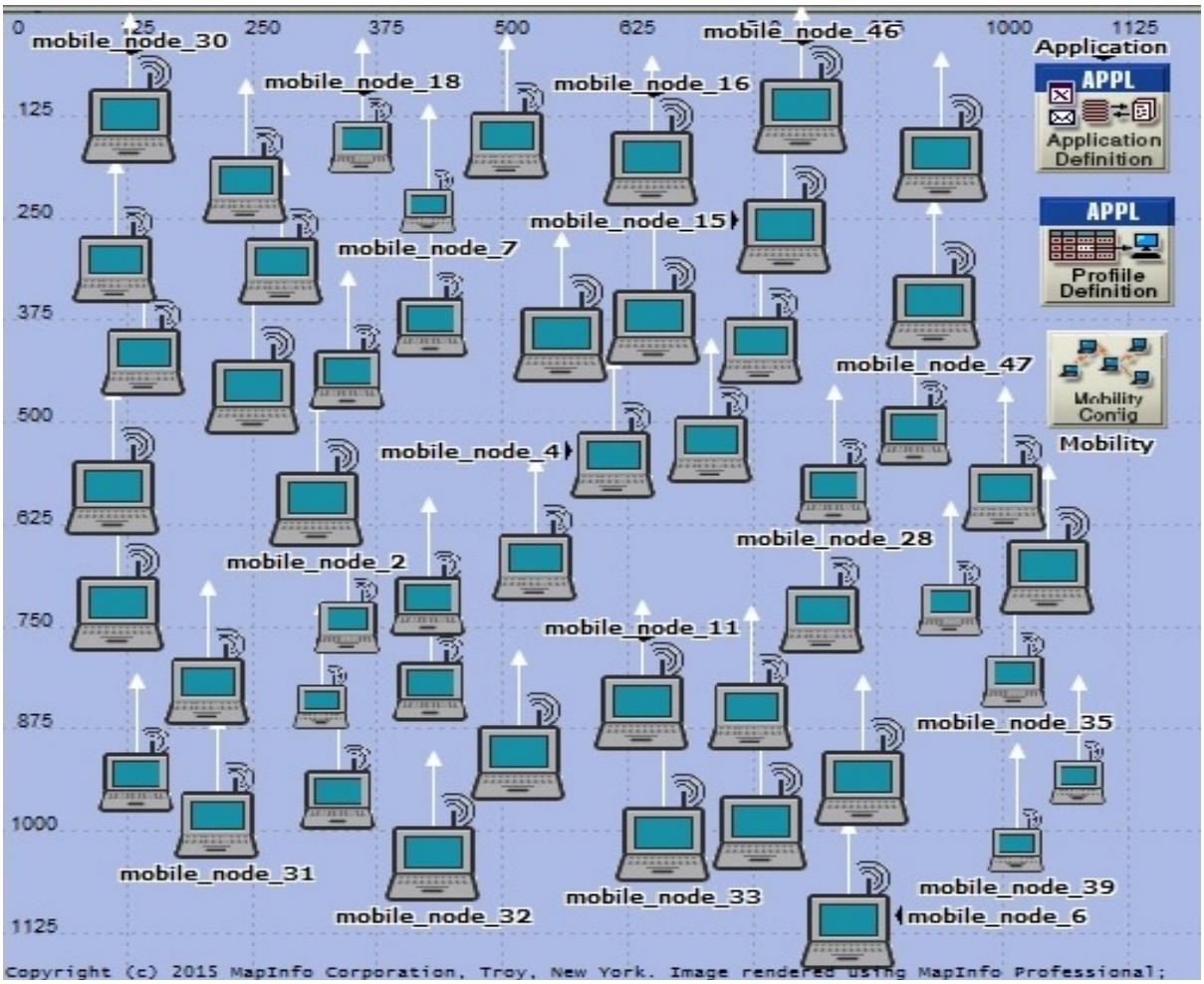

Figure 1. Simulation Scenario 1.

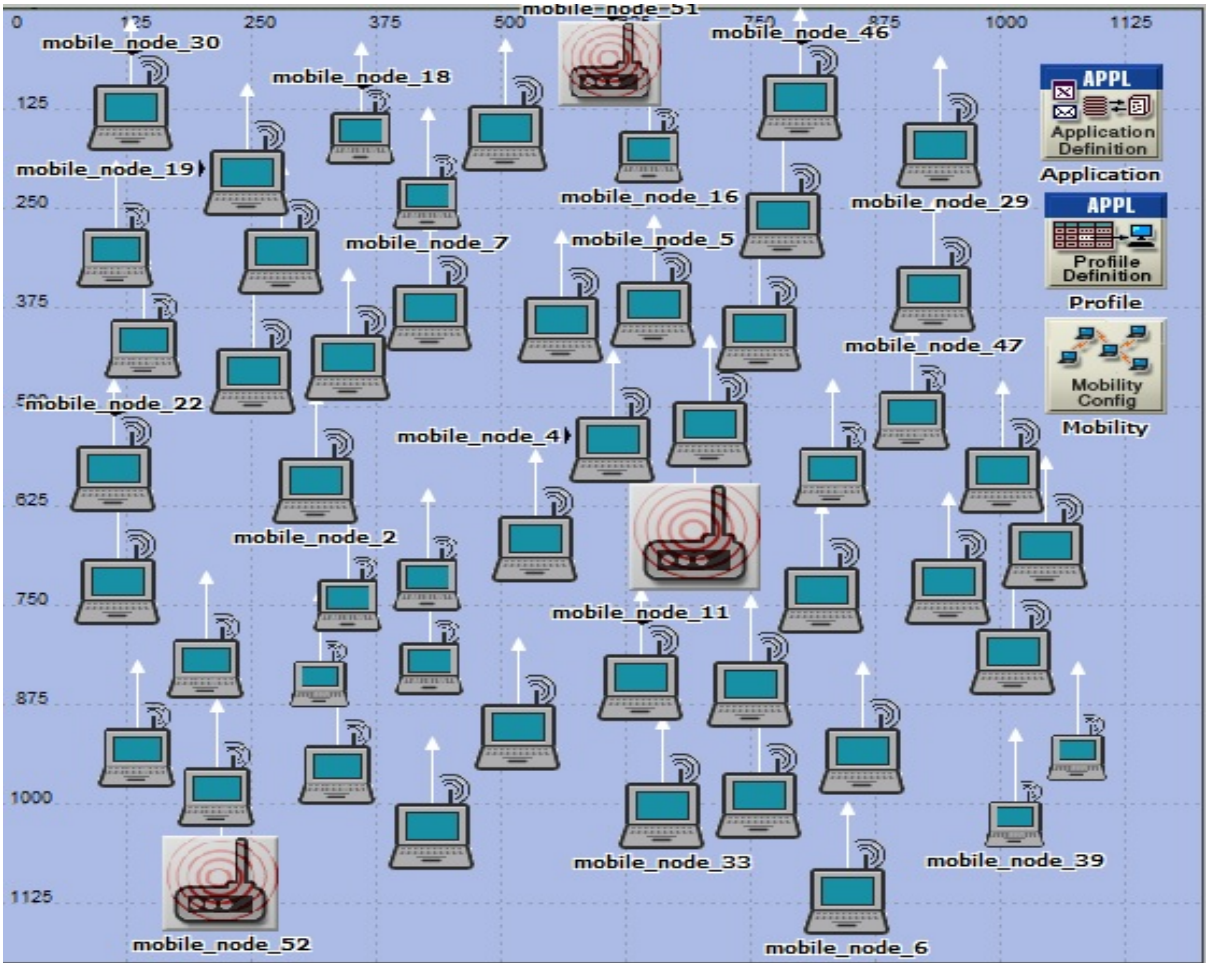

Figure 2. Simulation Scenario 2.

While these nodes attempting to communicate between each other properly, two jammer nodes violate communication. They constantly sent large size data packages to the network so that it causes less network throughput, collision occurrences and high network traffic. These jammer nodes were specified according to requirements of the project. Jammer nodes transmit data packages in large sizes. It sends constantly 10,000 bits size of data packages. In simulation model this jamming attack will keep being as long as the simulation continue. Therefore network communication is affected adversely.

All these circumstances directly affect network throughput. In scenario 2, these conditions have been simulated and evaluated. Comparison results of two scenarios clearly show how jamming attacks cause less throughput and high collision occurrence.

3.3. Performance Metrics

Simulation results are evaluated according to determined network performance criteria. In this experiment four performance metrics are taken. These metrics are Network Throughput, Network Load, WLAN Delay and Data Dropped. The network throughput refers to the amount of bits forwarded successfully from one network layer to another in a given time. Network throughput is typically measured as bits per second (bps), megabits in per second (Mbps) and gigabits per second (Gbps). On the other hand, Network Load is described as measurement of total data traffic on a WLAN Base Station Subsystem (BSS). It shows BSS load statistics of a network separately. Other performance metric which is WLAN Delay, represents latency of packages while they are travelling from one device to another. Finally Data Dropped statistics show total amount of data packages that are discarded by higher network level due to high buffer size of packages.

4. Simulation Results

Two scenarios have been subjected to simulation for one hour. In first scenario 50 mobile nodes had a proper communication between each other. There were not any malicious nodes or security attacks. These nodes have used MACAW protocol as collision avoidance protocol as well as they have used AODV protocol as mobile ad-hoc network routing protocol. Likewise scenario 1, scenario 2 had the same protocols, and equal number of mobile nodes. On the other hand unlike scenario 1, scenario 2 had also 3 mobile constant jammer nodes. Network model in scenario 2 was exposed to a powerful and constant jamming attack. These jammer nodes have sent large data packages to the network. In simulation results we have seen the performance of MACAW protocol under jamming attack condition. These 2 scenarios were simulated within a Discrete Event Simulation (DES) environment. Simulation outcomes and statistics were generated by OPNET Modeler 14.5 in graphical charts according to mentioned conditions.

4.1. Average WLAN Throughput Statistics

As stated before, Network Throughput refers to number of bits that are forwarded successfully one layer to another in a given time. Measurement for this statistics is used to be bits per second (bps). In this topic, two scenarios' throughput is compared to each other. It is expected that throughput of scenario 1 would be higher than scenario 2 because as mentioned in previous chapters, malicious nodes and security attacks directly affect overall network performance. OPNET Modeler 14.5 has provided throughput comparison of the two scenarios as a consequence of 1 hour simulation. In the following figure, WLAN Throughput statistics comparison of 2 scenarios is shown.

Figure 3 clearly illustrates average Wireless LAN Throughput comparison of two scenarios. In the first scenario which doesn't have any malicious nodes, it can be easily seen that bit transfer rate is above 8,000,000 bits per second. Under normal network conditions network throughput reaches up to approximately 7.7 Mbit. Second scenario which is represented by a red line in the figure shows that when network is exposed to a jamming attack its overall throughput rapidly decreased below 3000,000 bits per second. It can be clearly seen that jamming attack has a significant impact on overall network performance. It decreases throughput approximately three times.

4.2. Average Wireless LAN Delay Statistics

Wireless LAN Delay statistics represent package latency while they are transferring one layer to another. When network performance is low, package transmission slows down. In this case total network delay becomes high. In **Figure 4**, comparison graphics of scenarios for Wireless LAN Delay statistics can be seen.

Blue line which represents Scenario 1 shows that WLAN Delay rate is close to zero seconds. In normal network state, packages are delivered one layer to another without more delay. However in second scenario it can be seen that package delay have rapidly increased. Jamming attack caused a significant latency of packages.

4.3. Average Wireless Data Dropped Statistics

As discussed previously, data drop rate represents data packages that are discarded by higher level network layer. When buffer size of a data package is higher than determined acceptable value, network automatically drops the data package. As known, in Denial of Service attacks malicious nodes constantly send packages in large sizes to make network resources unavailable. As measure, network administrators adjust server nodes to drop these large size data packages. In simulation scenarios, "Large Packet Processing" option is set as "Drop" in order to protect the network against possible damages of large size packages. Below **Figure 5** shows average Wireless LAN Data Dropped statistics.

Figure 5 clearly shows data drop rate comparisons of two scenarios. As seen, red line which represents Scenario 2 is higher than blue line. Because jammer nodes send packages in 10,000 bits size and network directly drops them.

4.4. Average Wireless LAN Network Load Statistics

Network Load represents measurement of total amount of data over entire network. In **Figure 6** Wireless LAN Network Load statistics comparison of two scenarios is shown.

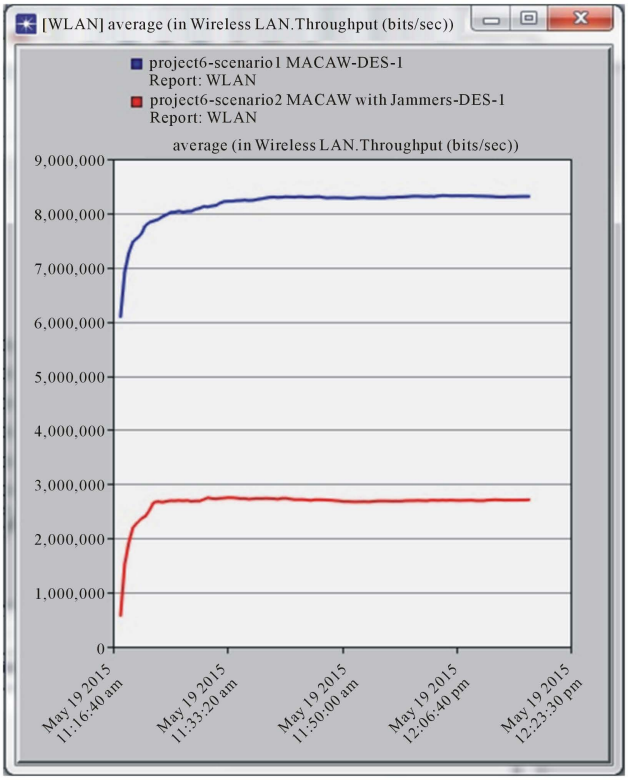

Figure 3. Average WLAN throughput comparison.

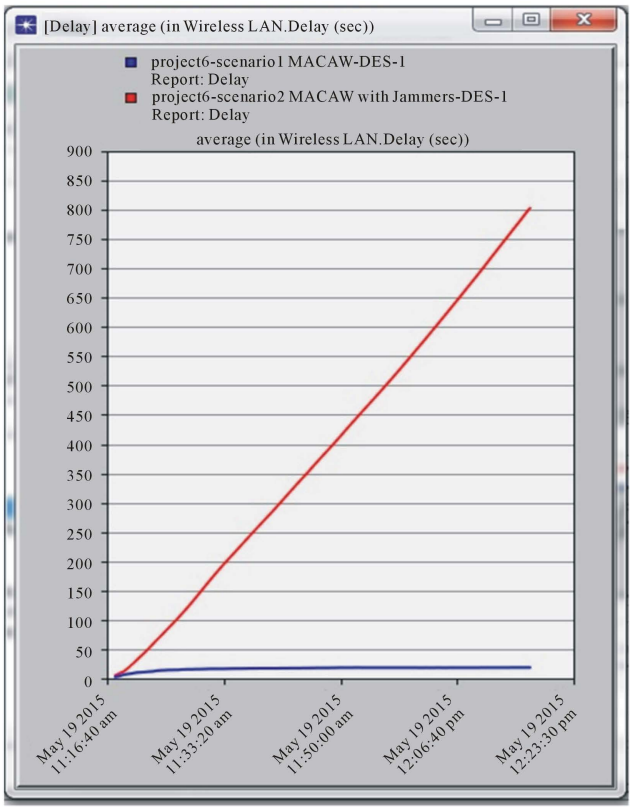

Figure 4. Average WLAN delay statistics.

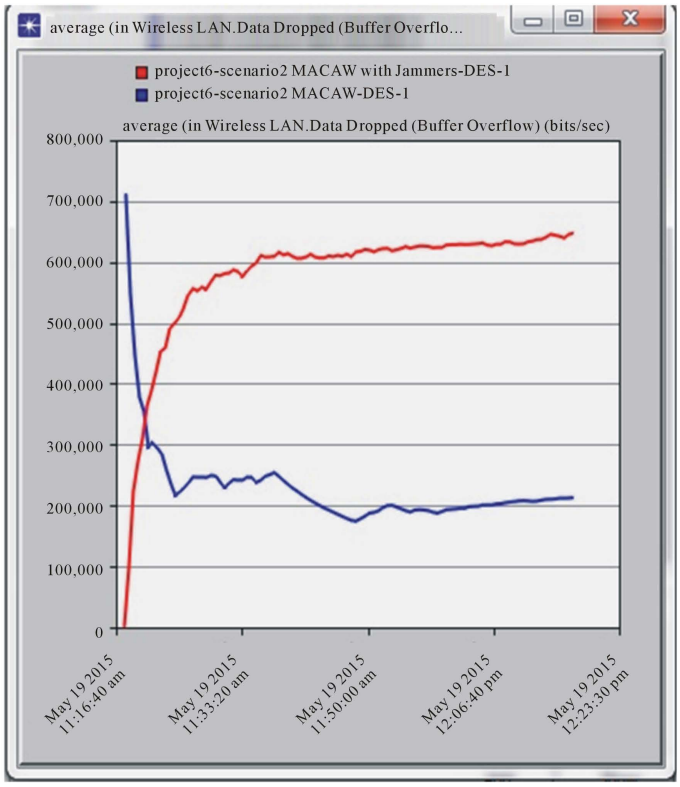

Figure 5. Average WLAN data dropped statistics.

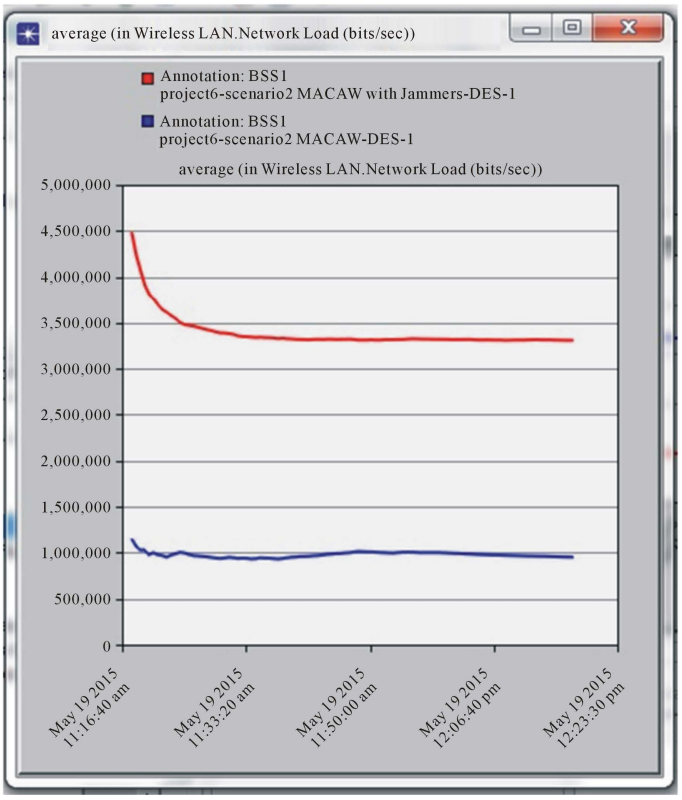

Figure 6. Average WLAN network load.

As it is shown through direct relationship between the average WLAN Data Dropped Rate on **Figure 5** and average WLAN Network Load on **Figure 6**, the scenario 2 had higher data dropped rate due to jamming attack and network load shown on **Figure 6** is higher due to injected packages into network through jammers. The huge amount of injected packages dropped from the network that is proven by the **Figure 5** with higher data dropped rate of scenario 2 and high network load value of **Figure 6** for scenario 2.

5. Conclusion

In the simulation case of study, the performance of MACAW protocol is evaluated. During this simulation, MACAW protocol has been exposed to a constant Jamming Attack. The main goal of this study is to observe possible impacts of a constant Jamming Attack on MACAW protocol. MACAW has shown a good performance unless it has been exposed to a Jamming Attack. It is seen in the simulation results that, a Jamming Attack in a mobile ad-hoc network leads to loss of performance of MACAW. Based on the simulation results, it can be claimed that Jamming Attacks cause approximately three times loss of network throughput where MACAW protocol is implemented. Delay rate in the network has significantly increased up to 800 seconds during Jamming Attack while it is close to zero second under normal network conditions. On the other hand, Data Dropped statistics show that 600,000 packages are discarded when MACAW is exposed to attack. In normal network conditions, this statistics is stable at the rate of 200,000 dropped data packages. In the jamming scenario, Network Load which is the final performance criteria shows that average load is at the rate of 4500,000 bits per second in the beginning of the simulation whereas it is stable at approximately 3500,000 bits per second at the end of the simulation. However, in the normal scenario Network Load statistics is stable at the rate of 1000,000 bits per second. Jamming Attack causes not only three times decrease in the network throughput but it also causes three times increase in the network load. This simulation experiment is the first study that deals with the performance evaluation of MACAW protocol under a constant Jamming Attack. Depending on results of our simulation experiment, it is strongly recommended other researchers to simulate performance of MACAW protocol under different security attacks such as Man in the Middle, Distributed Denial of Service and Spoof Attack. It is also recommended that precautions against attacks should be taken in MACAW protocol.

References

[1] Rouse, M. Collision Definition. http://searchnetworking.techtarget.com/definition/collision

[2] Obasuyi, G. and Sari, A. (2015) Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. *International Journal of Communications, Network and System Sciences*, **8**, 260-273. http://dx.doi.org/10.4236/ijcns.2015.87026

[3] Sharanappa, P.H. and Mahabaleshwar, S.K. (2014) Performance Analysis of CSMA, MACA and MACAW Protocols for VANETs. *International Journal of Future Computer and Communication*, **3**.

[4] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile Ad Hoc Networks. *International Journal of Science and Advanced Technology*, **2**, 188-191.

[5] Joa-Ng, M. (1999) Spread Spectrum Medium Access Protocol with Collision Avoidance in Mobile Ad-hoc Wireless Network. *INFOCOM*'99, *Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, **2**. http://dx.doi.org/10.1109/infcom.1999.751465

[6] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, **3**, 79-94.

[7] Zimmermann, H. (1980) OSI Reference Model—The IS0 Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications*, **COM-28**, 425-432. http://dx.doi.org/10.1109/TCOM.1980.1094702

[8] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET—Performance Evaluation of USM and RAS. *International Journal of Communications, Network, and System Sciences*, **7**, 365-372.

[9] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. *Transactions on Networks & Communications, Society for Science and Education, United Kingdom*, **2**, 1-6.

[10] Bharghavan, V., Demers, A., Shenker, S. and Zhang, L. (1994) MACAW: A Media Access Protocol for Wireless LAN's.

[11] Sari, A., Rahnama, B. and Caglar, E. (2014) Ultra-Fast Lithium Cell Charging for Mission Critical Applications. *Transactions on Machine Learning and Artificial Intelligence, United Kingdom*, **2**, 11-18.

[12] Pan, J. (2008) A Survey of Network Simulation Tools: Current Status and Future Developments. http://www.cse.wustl.edu/~jain/cse567-08/ftp/simtools.pdf

[13] Sari, A. (2015) Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, IGI Global, Hershey, 66-94. http://dx.doi.org/10.4018/978-1-4666-8345-7.ch005

[14] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *International Journal of Communications, Network and System Sciences*, **8**, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003

[15] Sari, A. and Onursal, O. (2013) Role of Information Security in E-Business Operations. *International Journal of Information Technology and Business Management*, **3**, 90-93.

[16] Sari, A. (2015) A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*, **6**, 142-154. http://dx.doi.org/10.4236/jis.2015.62015

[17] Sari, A. and Rahnama, B. (2013) Addressing Security Challenges in WiMAX Environment. *Proceedings of the* 6*th International Conference on Security of Information and Networks* (*SIN*'13), ACM, New York, 454-456. http://dx.doi.org/10.1145/2523514.2523586

[18] Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. 2013 *Fifth International Conference on Computational Intelligence, Communication Systems and Networks* (*CICSyN*), 5-7 June 2013, 334-337. http://dx.doi.org/10.1109/cicsyn.2013.79

[19] Rahnama, B., Sari, A. and Makvandi, R. (2013) Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial Data Interconnect. 2013 *International Conference on Technological Advances in Electrical, Electronics and Computer Engineering* (*TAEECE*), 9-11 May 2013, 579-582.

[20] Sari, A. (2015) Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite. *International Journal of Communications, Network and System Sciences*, **8**, 29-42. http://dx.doi.org/10.4236/ijcns.2015.83004