In this paper, a jamming attack (a kind of Denial-of-Service attack) was investigated, which interfered with the normal operation of a Mobile Ad Hoc network, which is more vulnerable to various attacks because of its self-configuration, dynamic characteristics, therefore, jammers would affect the network QoS parameters by reducing the throughput and increasing the delay. This problem is solved in this study by enabling the Point Coordination Function, which is a media access mechanism specified by the IEEE standard in some selected MANET nodes (guard nodes) to improve the deficiency of MANET's performance. The Riverbed modeler was utilized as a simulation tool. In this study, six jammers with two different transmission power values had been applied. In a number of different simulation scenarios with and without jammers, the estimated results showed that the jammers affected the network performance by increasing the delay to 3.0658 sec and decreasing the throughput to 120200.59 bits/sec. After enabling the PCF mechanism in a number of selected nodes, the results allowed the user to solve the problem by improving the network deficiency so that the throughput had been increased to 137478.32 bits/sec and the delay had been decreased to 0.7556 sec. It can be concluded that PCF is a good improvement for different levels of jammer transmission power such as 0.01 W and 0.001 W, and PCF also improved the network's delay and throughput when the number of PCF enabled nodes had been increased to 10 nodes and 12 nodes, respectively. The improvement is also increased. This study can be used in practice for any ad hoc network when attacked by jammers

Keywords: MANET, Riverbed, point coordination, routing protocols, jamming attacks, delay, throughput

UDC 004
DOI: 10.15587/1729-4061.2022.265779

POINT COORDINATION MECHANISM BASED MOBILE AD HOC NETWORK INVESTIGATION AGAINST JAMMERS

Shayma W. Nourildean
Corresponding author
Master of Engineering, Lecturer
Department of Computer Technical Engineering
University of Technology — Iraq
Alsinaa str., Baghdad, Iraq, 00964
E-mail: Shayma.w.nourildean@uotechnology.edu.iq
Sabbar I. Jasim
Master of Engineering, Lecturer
Department of Computer Technical Engineering
Dijlah University
Durah Masafi str., Baghdad, Iraq, 00964
May T. Abdulhadi
Master of Engineering, Assistant Lecturer
Iraqi Commission for Computers and Informatics
Almansour str., Baghdad, Iraq, 00964
Mustafa Musa Jaber
PhD, Lecturer
Institute of Informatics and Computing
in Energy, Universiti Tenaga Nasional
Jl. Ikram-Uniten, Selangor, Malaysia, 43000
Al-Farahidi University
Qetr Alnada str., Baghdad, Iraq, 10020

Received date 09.08.2022
Accepted date 12.10.2022
Published date 27.10.2022

How to Cite: *Nourildean, S. W., Jasim, S. I., Abdulhadi, M. T., Jaber, M. M. (2022). Point coordination mechanism based mobile ad hoc network investigation against jammers. Eastern-European Journal of Enterprise Technologies, 5 (9 (119)), 45–53. doi: https://doi.org/10.15587/1729-4061.2022.265779*

1. Introduction

Wireless networks have recently become a major topic in the wireless communications area. These networks can be used in a variety of technological domains, including industry, the military and personal area networks. In contrast to wired networks, wireless networks such as Wi-Fi, satellite communication systems, and cellular phone networks do not require established infrastructure. They consist of a collection of mobile and wireless nodes that dynamically exchange data without the use of infrastructure such as a base station or an access point. A network node has two functions: it serves as a client and vendor of data packets, as well as a router for data packets sent to other nodes [1]. MANET nodes can join and exit the network at any time. In the event that the source node is not immediately accessible to the destination node, these nodes can employ multi-hop communication. The collaboration of intermediary nodes is required for node dependability. As a result, MANET designs are vulnerable to a variety of assaults [2]. MANET manages a variety of sensitive data from a variety of applications in a variety of industries, making it more vulnerable to diverse attacks owing to its dynamic nature. The nodes in the network are self-configuring, therefore, they can travel from one location area to another freely without the need for centralized management [3]. Therefore, the studies that are devoted to improving MANET against jammers utilizing PCF are scientifically relevant in the modern times for the study or design of any ad hoc network because the self-organized nature of MANET made it valnerable to jammers, which cause network deficiency. So, the results of these studies could improve the quality of service parameters of the network performance.

2. Literature review and problem statement

In [4], the performance of mobile ad hoc networks under jamming was studied. This project contains a high-mobility

network built with the IEEE g standard and optimized AODV routing protocol settings using OPNET (Optimized Network Engineering Tool) Modeler 14.5 simulation for video conferencing and FTP applications with high data rates in terms of QoS criteria such as network load, retransmission attempts, media access latency, and so on. Jamming attacks have been demonstrated to affect network performance, retransmission efforts, and media access latency. The solution of this problem remains unexplored, so this research studies the jammer effect on network performance. In [5], JR-SND had been proposed, a secure neighbor finding method for MANETs that is jamming-resistant and is based on random spread-code predistribution and direct-sequence spread spectrum. Despite the constant presence of jammers, JR-SND enables neighboring nodes to securely discover one another with a high probability but the problem with this study is the difficulty to implement. The researchers in [6] propose an approach for detecting predicted jamming attacks by utilizing statistical process control on the packet drop ratio (PDR), which is the number of dropped packets divided by the total number of packets delivered. It had been concluded that the control chart for fractional nonconforming based on the PDR helped to detect the jammer assault in real time via a visual graph as the performance had been evaluated. The problem with this research is that the metric's assimilation reveals the nonconforming percentage. The work [7] presented a probabilistic framework based on the location of jammed and unjammed nodes for identifying jammers. In a multi-jammer scenario, we are looking for the lowest set of nodes that can be eliminated in order to thwart attacks. The researchers in this study demonstrated the NP-hardness of this problem and suggested a polynomial-time heuristic approach for approximating solutions. The work [8] proposed MAC protocols and jamming-aware routing for a number of jamming scenarios, where the jamming schedule is known to the friendly mobile nodes but hidden from all adversarial ones. The outcomes showed that the proposed protocols can significantly improve the packet delivery ratio and other metrics. The paper [9] proposed a policy-based harmful peer detection technique in which context data such as communication channel status, transmission power level and buffer status are gathered in order to determine whether or not the misbehavior is likely the consequence of malicious activity. The simulation findings show that the policy-based harmful peer detection approach can reliably distinguish malicious peers from defective peers. Furthermore, with a low communication cost, the technique converges to an equal view of harmful nodes among all nodes, but the collected data do not confirm whether the misbehavior is an outcome of malicious activity or not. The project in [10] discussed the same problem but as a review so that MANETs, different forms of jamming assaults had been examined, and jamming attacks in wireless sensor networks had been classified. The work's main contribution is the accurate and low-false-alarm categorization of jammers. The network's performance will be harmed as the jammer reduces throughput and increases latency. This approach was used in [11] to examine some of the key issues of security attacks in mobile ad hoc networks, as well as some of the existing mitigation systems. Taguchi's loss function had been utilized to determine the network's performance degradation in the existence of a security scheme. This effort reduces network overhead by improving maximum drop dependent parameters. This research showed that Taguchi's loss function is able to improve the network performance as a good solution. The suggested approach in [12] enhances detection accuracy and packet delivery ratio, taking into account a number of critical elements, including packet delivery ratio (PDR), signal intensity (SS) and carrier sensing time. Then, for each node, a trust model is created and updated. The jammer had been detected by checking the updated trust values of a suspicious node but the relevance of this research might be impractical. The approach used in [13] suggested a new method for detecting and isolating malicious nodes from a network. Monitor mode and threshold will be used in the suggested approach. The simulation was run in NS2, and the results show that the suggested approach works well in terms of data dropped, delay, PDR and throughput but it is difficult to implement this approach in the real world. The approach used in [14] introduced swarm intelligent algorithms like the Enhanced Ant Colony Optimization (EACO) and Enhanced Artificial Bee Colony (EABC) Algorithms as the primary contribution of the current research study to solve the jamming attack problem but the jammers used in this research are an academic model. These swarm intelligence algorithms are more adaptable and increase the algorithms' capacity for searching.

However, all this allows us to assert that it is expedient to conduct a study on using a Point Coordination mechanism in some nodes of any ad hoc network to solve the problem of the network deficiency caused by jammers.

3. The aim and objectives of the study

The aim of this study is to develop point coordination mechanism based mobile ad hoc network investigation against jammers. This will make it possible to improve the efficiency of the network in terms of delay and throughput and thus would increase the network speed.

To achieve this aim, the following objectives are accomplished:

– to measure delay and throughput in the three cases (without Jammers, Jammers and Jammers with PCF when the jammer transmission power is equal to 0.001 W and the PCF was enabled in 8 nodes;

– to measure delay and throughput in the three cases (without Jammers, Jammers and Jammers with PCF when the jammer transmission power is equal to 0.01 W and the PCF was enabled in 8 nodes;

– to measure delay and throughput in the three cases (without Jammers, Jammers and Jammers with PCF when the jammer transmission power is equal to 0.01 W and the PCF was enabled in 10 nodes;

– to measure delay and throughput in the three cases (without Jammers, Jammers and Jammers with PCF when the jammer transmission power is equal to 0.01 W and the PCF was enabled in 12 nodes.

4. Materials and methods

4. 1. Object and hypothesis of the study

The object of the study is an ad hoc network utilizing the point coordination mechanism. The research subject is to increase the efficiency of the network because jammers interfered with the normal operation of the network and caused network deficiency. The assumption made in the work is that a number of jammers interfere with the normal operation of the mobile ad hoc network and reduced the throughput, as well as increased the delay.

The main hypothesis of the study is that PCF is enabled in some nodes in the network to study how it would improve the performance of the network. This network is modeled and simulated utilizing Riverbed Modeler v17.5 because it is an active software to create and simulate a variety of network devices, kinds, and protocols in an efficient, simple and flexible way.

4. 2. Theoretical basis

The theoretical basis of this paper would be in terms of:

a) mobile ad hoc network.

MANET is a self-contained mobile nodes network with routing abilities that are linked through wireless networks. Every mobile node has the ability to operate as a router and connect with other nodes in its physical neighbors. MANETs are characterized by autonomous self-configuration, self-maintenance, low deployment costs, and the absence of fixed network infrastructures or centralized management, so that it is an information exchange network made up of mobile nodes that can change positions dynamically [15, 16]. Fig. 1 illustrates a simple MANET topology [17].

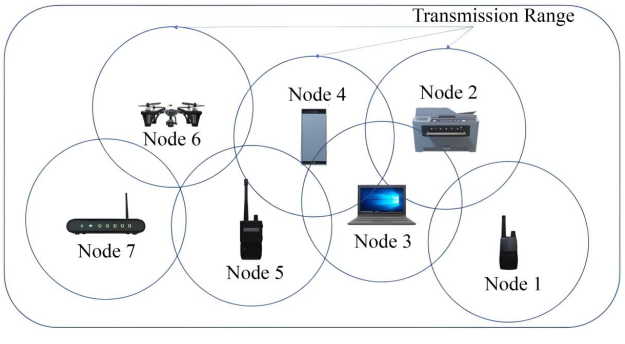

Fig. 1. Mobile ad hoc network topology [17]

b) classification of attacks in the mobile ad hoc network.

MANET is more vulnerable to various attackers due to its dynamic characteristics, self-configuration and nodes in the network can move freely from one location to another without any central control, therefore, the routing of data must be secured to discover, block, and respond to security assaults [3, 10]. Classification of security attacks by type is shown in Fig. 2 [18].

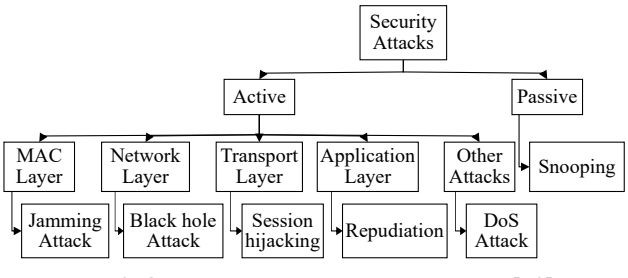

Fig. 2. Security attacks for different layers [18]

c) jamming attack.

In MANET, jamming is a severe danger to its security. A jamming assault sends out radio signals with the goal of disrupting all communications by lowering the signal to noise ratio. The word jamming is used to distinguish it from interference, which involves unintended jamming [4]. The jammer is an entity that interferes with the transmission and reception of data via network's wireless communications [19]. A heavily pushed signal of comparable frequency disrupts an ad hoc communication channel [20]. Jamming attacks have a number of characteristics in common, including the use of MAC protocols to communicate. This paper examined the impact of a number of jammers on a MANET, which reduces the network efficiency by affecting the QoS parameters of the network. In this paper, the PCF mechanism was utilized to improve the network performance. The amming attack is shown in Fig. 3.

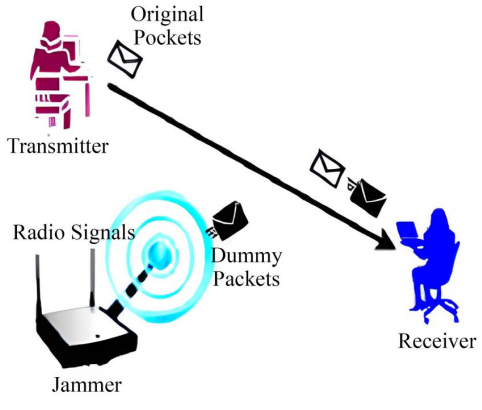

Fig. 3. Jamming attack [4]

d) point coordination function (PCF).

Point coordination function (PCF) and Distributed coordination function (DCF) are the two different IEEE 802.11 standard media access control (MAC) mechanisms. PCF is built on the top of and provides media access, which is free of contention, therefore, PCF can achieve higher throughput than contention-based DCF. PCF could improve deficiency caused by jammers [21, 22]. In the PCF, the centralization of wireless channel access is a protocol based on polling, which is controlled by the central point called point coordinator (PC). The access point serves as PCs. The PCF is shown in Fig. 4 [23].

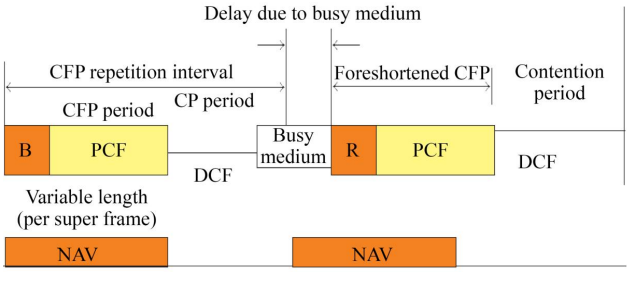

Fig. 4. Point coordination function mode of operation [23]

This paper improves the MANET deficiency caused by jammers.

4. 3. Research method

MANETs are characterized by their mobility. Experimentation is largely possible through simulation due to the high cost and lack of flexibility of such real networks. Riverbed Modeler simulation tool is an active software that allows users to create and simulate a variety of network devices, kinds, and protocols in an efficient and flexible way. Riverbed Modeler has a graphical user interface for building, developing and simulating different networks allowing users to

monitor and collect the network data right away in consistent simulated results [24–26].

4. 4. Simulation setup

In this research, the problem is that jammers interfered with the network, which caused the network deficiency by increasing the delay and thus slowing the network speed and decreasing the throughput. The solution was investigated by enabling PCF in some selected nodes for different transmission power of jammers. The simulation of PCF-based MANET with jammers consists of five modeled scenarios utilizing Riverbed Modeler 17.5. The steps of the simulation setup are as follows:

1. Each scenario had 30 MANET stations connected wirelessly to a wireless server.

2. Define profile configuration and application configuration to define the required applications and assign these applications and services to the profile of each object.

3. Six jammers were applied in some of the modeled scenarios for this study.

4. Point Coordination Function (PCF) is enabled in 8 nodes, 10 nodes and 12 nodes to improve the QoS parameters of the network as a solution to the problem of network deficiency by jammers.

5. There are three types of MANET in Riverbed Modeler as shown in Fig. 5.

6. The nodes of this simulation are shown in Table 1.

7. Choosing the network statistics in terms of delay and throughput.

8. The simulation is run for 20 minutes.

9. The results were collected.

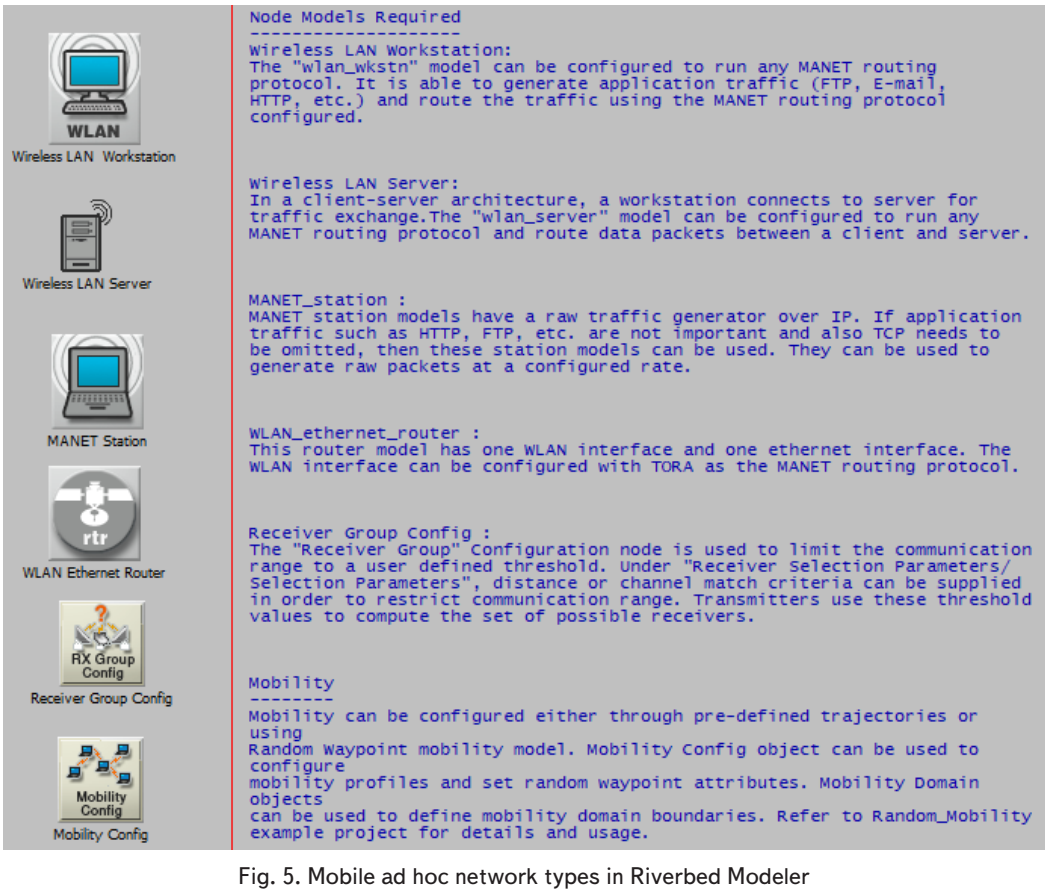

Fig. 5. Mobile ad hoc network types in Riverbed Modeler

Table 1

Network simulation objects

WLAN workstation running any proactive MANET routing protocol	30
Wireless LAN server running any proactive MANET routing protocol	1
Jamming Attack (Jammer)	6
Profile, Application and Mobility configuration	1
Applications	HTTP, Video, File Transfer and Mobile Instant Messaging
Wi-Fi Data transfer	24 Mbps
Transmission Band	2.4 GHz
Transmission Power of the MANET node	0.005 Watt
Repeatability	Unlimited
Operation mode	Serial (ordered)
Simulation duration	1,200 sec

The scenarios are as follows:

1. Scenario 1 named MANET without Jammers: this scenario had 30 MANET stations connected wirelessly to the server without any jammers as shown in Fig. 6.

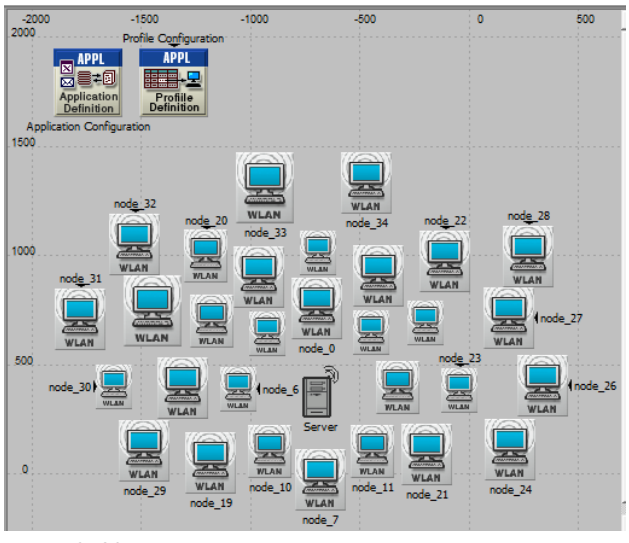

Fig. 6. 30 mobile ad hoc network nodes without jammers

2. Scenario 2 named MANET with Jammers P1: in this scenario, six jammers interfered with the network with a transmission power=0.001 W and the specification of the jammers is shown in Fig. 7.

This scenario is shown in Fig. 8.

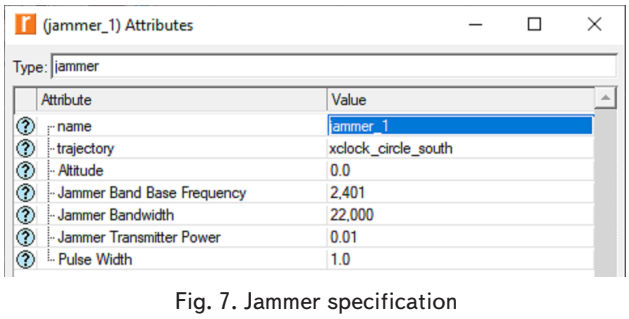

Fig. 7. Jammer specification

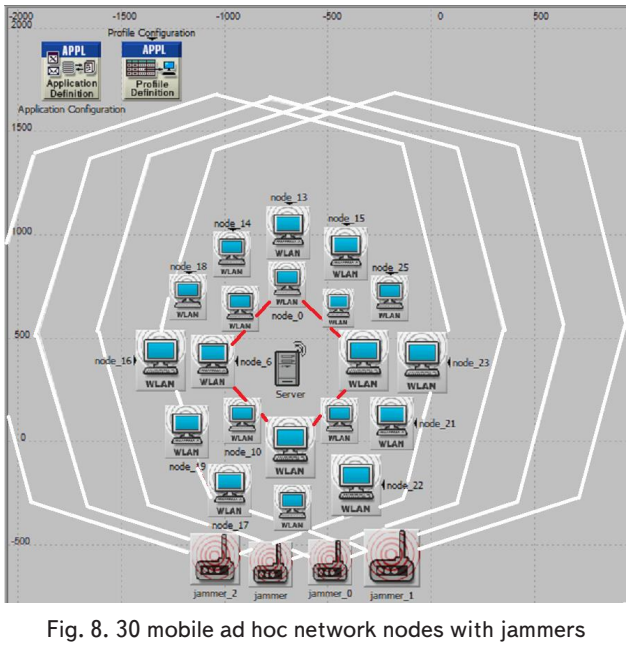

Fig. 8. 30 mobile ad hoc network nodes with jammers

3. Scenario 3 named MANET with Jammers 8 PCF P1: in this scenario, the PCF mechanism is applied to the selected MANET nodes (8 nodes) to improve the network deficiency caused by jammers at the jammer transmission power of 0.001 W. This specification of the PCF mechanism is shown in Fig. 9.

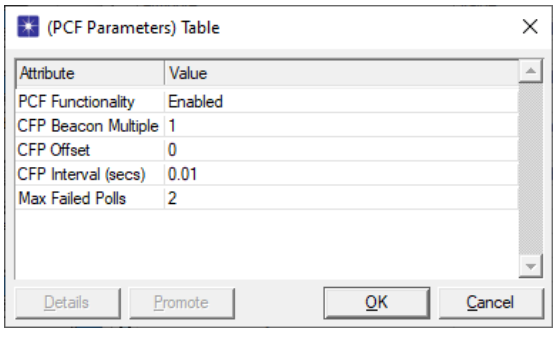

Fig. 9. Point coordination function specification

4. Scenario 4 and Scenario 5 named MANET with Jammers P2 and MANET with Jammers 8 PCF P2: in these two scenarios, the transmission power of each jammer was increased to 0.01 W to show the role of PCF with different levels of jammer transmission power.

5. Scenario 6 and Scenario 7 named MANET with Jammers 10 PCF P2 and MANET with Jammers 12 PCF P2: in these scenarios, the number of nodes with enabled PCF was increased to 10 and 12 nodes, respectively, to show the PCF role when the number of selected PCF nodes was increased and the transmission power of each jammer is 0.01W.

4. 5. Performance metrics

The quality of service parameters were examined in each scenario of each network to study the performance of any network.

In this work, the statistics had been selected in terms of QoS parameters (Delay and Throughput) for the required applications:

1. Throughput: it is the number of bits transmitted per second.

2. Delay: it is all data packets' end to end delay, with which they are received from the MANET nodes to the higher levels.

The simulation had been run for 20 minutes.

5. Results of the mobile ad hoc network study

5. 1. QoS parameters with transmission power=0.001 W

In this study, two QoS parameters (delay and throughput) were investigated, which are important parameters to improve the performance of the network in order to achieve the aim of the project, which is the improvement of the network deficiency because the jammers increased the delay and decreased the throughput as shown below.

Throughput and delay of MANET without jammers were taken with the two scenarios of MANET with jammers and MANET with jammers and PCF when the transmission power of the jammer is 0.001 W.

The throughput and delay are shown in Fig. 10, 11, respectively. Then, the transmission power had been increased to 0.01 W.

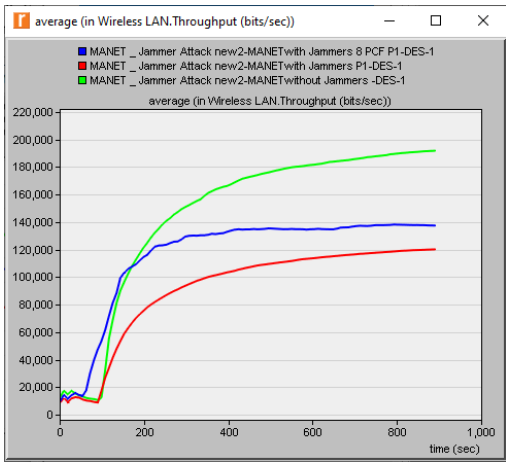

Fig. 10. Throughput (30 nodes, 8 PCF nodes, Transmission Power=0.001 W)

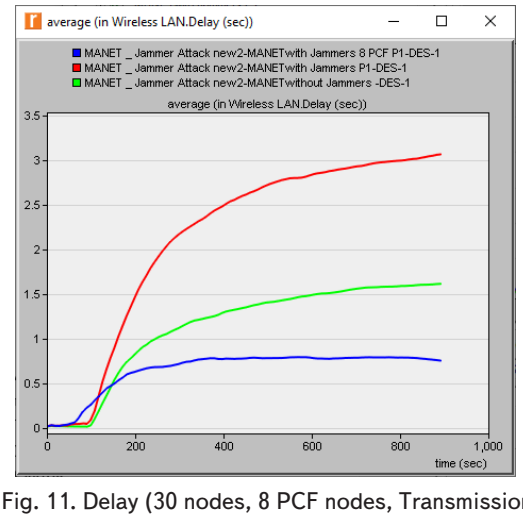

Fig. 11. Delay (30 nodes, 8 PCF nodes, Transmission Power=0.001 W)

5. 2. QoS parameters with transmission power=0.01 W

Throughput and delay of MANET without jammers with the two scenarios of MANET with jammers and MANET with jammers and PCF when the transmission power of the jammer is increased to 0.01 W are shown in Fig. 12, 13, respectively.

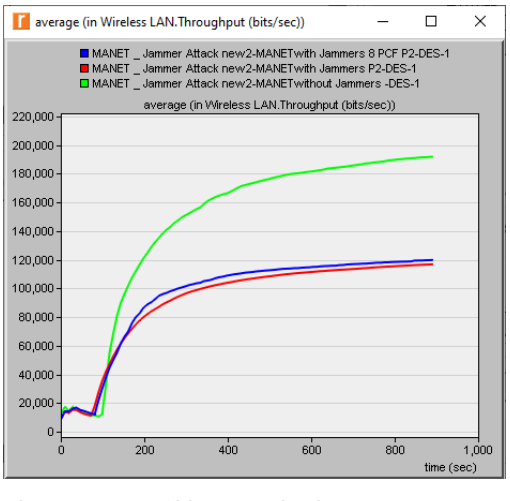

Fig. 12. Throughput (30 nodes, 8 PCF nodes, Transmission Power=0.01 W)

Then, the number of PCF enabled nodes had been increased to 10 nodes.

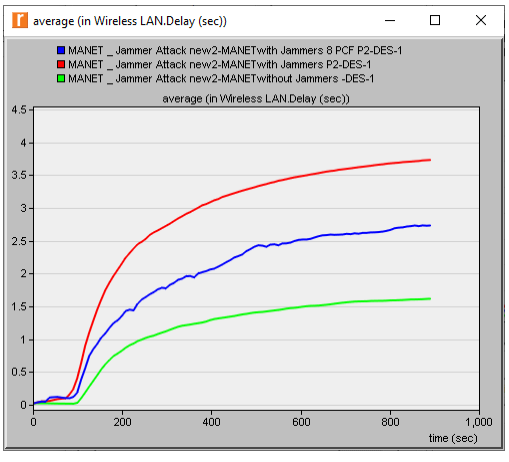

Fig. 13. Delay (30 nodes, 8 PCF nodes, Transmission Power=0.01 W)

5. 3. QoS parameters with transmission power=0.01W and 10 PCF nodes

Throughput and delay when the number of PCF enabled had been increased to 10 nodes and the transmission power is 0.01 W are shown in Fig. 14, 15, respectively.

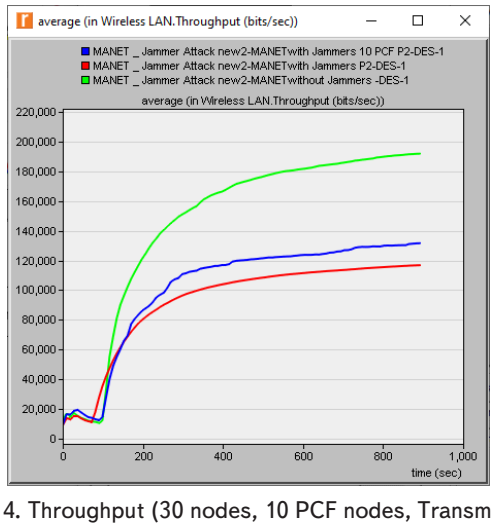

Fig. 14. Throughput (30 nodes, 10 PCF nodes, Transmission Power=0.01 W)

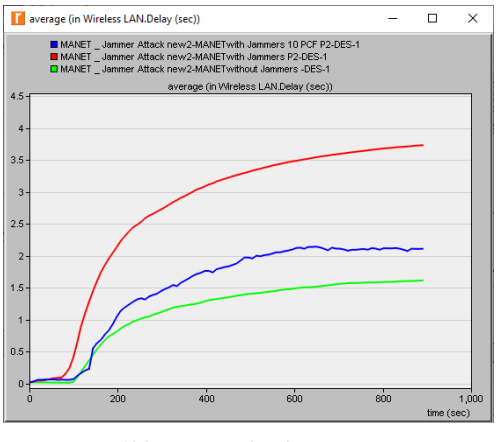

Fig. 15. Delay (30 nodes, 10 PCF nodes, Transmission Power=0.01 W)

Then, the number of PCF enabled nodes had been increased to 12 nodes.

5. 4. QoS parameters with transmission power=0.01 W and 12 PCF nodes

Throughput and delay when the number of PCF enabled nodes had been increased to 12 nodes and the transmission power is 0.01 W are shown in Fig. 16, 17, respectively.

The summary of the simulation results is shown in Table 2.

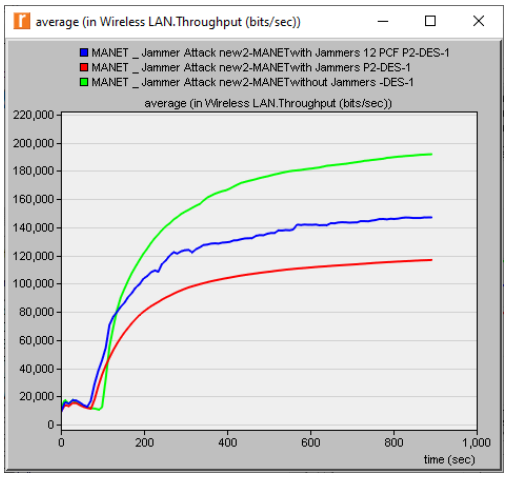

Fig. 16. Throughput (30 nodes, 12 PCF nodes, Transmission Power=0.01 W)

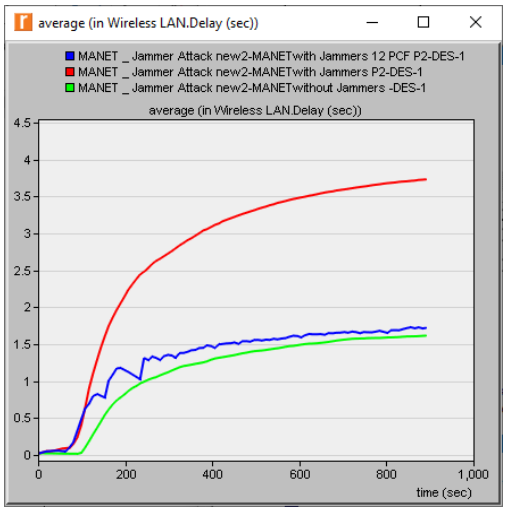

Fig. 17. Delay (30 nodes, 12 PCF nodes, Transmission Power=0.01 W)

In the following section, a discussion of the results of the study is presented for conclusion.

6. Discussion of delay and throughput results

After the network is built and simulated in the Riverbed Academic Edition v17.5 platform, the simulation had been run and the results were collected. Jammers with a transmission power of 0.001 W affect the network because they reduced the throughput and increased the delay of the MANET as shown in Fig. 10, 11. These delay and throughput QoS parameters are the major drawback of the network performance. The previous work examined MANET Routing protocols performance under jamming attacks. Some researches detect jamming attacks utilizing different methods. The aim of this work is to examine how this MANET could be improved from the drawback caused by the jammers using the Point coordination function (PCF), which is a media access mechanism specified by the IEEE 802.11 standard. The PCF mechanism is enabled in eight nodes so that it had improved the deficiency of the network and the delay had been decreased and the throughput and the speed had been increased slightly. The network is modeled in different scenarios with the number of MANET nodes connected to the server. The jammer with a transmission power of 0.001 W entered the network and interfered with the normal operation of the network and thus decreasing the throughput and increasing the delay so that slowing the network speed indicated by the red line in Fig. 10, 11. In this study, PCF is enabled in eight selected nodes to solve the network deficiency problem so that the throughput and delay had been improved as shown in Fig. 10, 11, respectively. Then, the jammer interfered with the network with a transmission power of 0.01 W. In terms of delay, PCF enabled nodes achieved a good improvement as indicated by the blue line as shown in Fig. 13, but had no throughput improvement as shown in Fig. 12. Then, the number of PCF enabled nodes had been increased to 10 nodes, throughput improvement as well as delay improvement had been investigated as indicated by blue lines in Fig. 14, 15, respectively. Then, the number of PCF enabled nodes had been increased to 12 nodes for an extra throughput improvement as well as delay improvement as indicated by blue lines in Fig. 16, 17, respectively. As seen above, as the number of PCF enabled nodes had been increased to 12, the delay reached the delay without jammers, which is an excellent performance as well as an extra improvement in throughput.

Table 2

Summary of Simulation Results

Jammer	Parameter \ Network Scenario	MANET without Jammers	MANET with Jammers	MANET with Jammers and PCF
Jammer Transmission Power=0.001 W with 8 PCF nodes	Throughput	1918,87.58	120,200.59	137,478.32
	Delay	1.6161	3.0658	0.7556
Jammer Transmission Power=0.01 W with 8 PCF nodes	Throughput	191,887.58	116,819.43	119,890.45
	Delay	1.6161	3.7312	2.7324
Jammer Transmission Power=0.01 W with 10 PCF nodes	Throughput	191,887.58	116,819.43	131,616.96
	Delay	1.6161	3.7312	2.1112
Jammer Transmission Power=0.01 W with 12 PCF nodes	Throughput	191,887.58	116,819.43	147,049.87
	Delay	1.6161	3.7312	1.7204

The limitation of PCF is that 802.11 MAC didn't include any admission control mechanism to provide access priority to the wireless medium but this study had no limitation when trying to be applied in practice. The development of this research lies in the use of a suitable MANET routing protocol, which played a significant role in the improvement of network efficiency.

7. Conclusions

1. Delay and Throughput in the three cases (without Jammers, Jammers, and Jammers with PCF) had been measured when the transmission power of the jammer is equal to 0.001 W and the PCF was enabled in 8 nodes. With quantitative indicators of the research results, the point coordination mechanism (PCF) improved the MANET performance by decreasing the delay and increasing the throughput, which solved the problem of network deficiency caused by jammers.

2. Delay and Throughput in the three cases (without Jammers, Jammers, and Jammers with PCF) had been measured when the transmission power of the jammer is increased to 0.01 W and the PCF was enabled in 8 nodes. With quantitative indicators of the research results, the point coordination mechanism (PCF) improved the MANET performance in terms of delay, which solved the delay problem of network deficiency caused by jammers but it had no throughput improvement.

3. Delay and Throughput in the three cases (without Jammers, Jammers, and Jammers with PCF) had been measured when the transmission power of the jammer is increased to 0.01 W and the PCF was enabled in 10 nodes. With quantitative indicators of the research results, the point coordination mechanism (PCF) improved the MANET performance in terms of delay and throughput, which solved the problem of network deficiency caused by jammers.

4. Delay and Throughput in the three cases (without Jammers, Jammers, and Jammers with PCF) had been measured when the transmission power of the jammer is increased to 0.01 W and the PCF was enabled in 12 nodes. With quantitative indicators of the research results, the point coordination mechanism (PCF) provides delay and throughput improvement so that the delay would reach the case of the network without jammers, which is a very good improvement that solved the problem of network deficiency caused by jammers.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

References

1. Alani, S., Zakaria, Z., Lago, H. (2019). A new energy consumption technique for mobile ad hoc networks. International Journal of Electrical and Computer Engineering (IJECE), 9 (5), 4147. doi: https://doi.org/10.11591/ijece.v9i5.pp4147-4153
2. Meddeb, R., Triki, B., Jemili, F., Korbaa, O. (2017). A survey of attacks in mobile ad hoc networks. 2017 International Conference on Engineering & MIS (ICEMIS). doi: https://doi.org/10.1109/icemis.2017.8273007
3. Vidhya Lakshmi, G., Vaishnavi, P. (2022). An Efficient Security Framework for Trusted and Secure Routing in MANET: A Comprehensive Solution. Wireless Personal Communications, 124 (1), 333–348. doi: https://doi.org/10.1007/s11277-021-09359-2
4. Singh, J., Gupta, S. (2017). Impact of Jamming Attack in Performance of Mobile Ad hoc Networks. International Journal of Computer Science Trends and Technology (IJCST), 5 (3), 184–190. Available at: http://www.ijcstjournal.org/volume-5/issue-3/IJCST-V5I3P33.pdf
5. Zhang, R., Sun, J., Zhang, Y., Huang, X. (2015). Jamming-Resilient Secure Neighbor Discovery in Mobile Ad Hoc Networks. IEEE Transactions on Wireless Communications, 14 (10), 5588–5601. doi: https://doi.org/10.1109/twc.2015.2439688
6. Houssaini, M.-A. E., Aaroud, A., Hore, A. E., Ben-Othman, J. (2016). Detection of Jamming Attacks in Mobile Ad Hoc Networks Using Statistical Process Control. Procedia Computer Science, 83, 26–33. doi: https://doi.org/10.1016/j.procs.2016.04.095
7. Albanese, M., De Benedictis, A., Jajodia, S., Torrieri, D. (2014). A probabilistic framework for jammer identification in MANETs. Ad Hoc Networks, 14, 84–94. doi: https://doi.org/10.1016/j.adhoc.2013.11.007
8. Kim, J., Biswas, P. K., Bohacek, S., Mackey, S. J., Samoohi, S., Patel, M. P. (2021). Advanced protocols for the mitigation of friendly jamming in mobile ad-hoc networks. Journal of Network and Computer Applications, 181, 103037. doi: https://doi.org/10.1016/j.jnca.2021.103037
9. Akila, R., Jenefer, M. P. (2016). Efficient Policy based Detection of Jamming Attacks in MANETS. International Journal of Advanced Research in Computer and Communication Engineering, 5 (3), 316–324. Available at: https://www.ijarcce.com/upload/2016/march-16/IJARCCE%2078.pdf
10. Maheswari, R., Rajeswari, S. (2015). A Review on Types of Jamming Attack In Mobile Ad-Hoc Network. Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications, 84–86. Available at: https://www.ijana.in/Special%20Issue/file18.pdf
11. Thapak, S., Chouksey, P. (2019). Protection From Jamming Attack And Service, Quality Improvement Of Network In Future MANET Communication Network. International Journal of Scientific & Technology Research, 8 (11), 3706–3714. Available at: http://www.ijstr.org/final-print/nov2019/Protection-From-Jamming-Attack-And-Service-quality-Improvement-Of-Network-In-Future-Manet-Communication-Network.pdf
12. Jayanand, A. (2020). A cooperative combined defense technique for jamming attack in MANET. International Journal of Operational Research, 37 (4), 549. doi: https://doi.org/10.1504/ijor.2020.105767

13. Aditi, Singh, J. K. (2017). Detection and isolation mechanism of jamming attack for aodv in manet. International Journal of Technical Research & Science, 2 (II), 76–83. Available at: https://www.ijtrs.com/uploaded_paper/DETECTION%20AND%20ISOLATION%20MECHANISM%20OF%20JAMMING%20ATTACK%20FOR%20AODV%20IN%20MANET%201.pdf
14. Vijayalakshmi, K., Hema Rajini, N. (2021). Detection Of Jamming Attack In Manet Using Enhanced Artificial Bee Colony Algorithm. International Journal of Electrical Engineering and Technology (IJEET), 12 (4), 25–32. Available at: https://iaeme.com/MasterAdmin/Journal_uploads/IJEET/VOLUME_12_ISSUE_4/IJEET_12_04_004.pdf
15. Sirmollo, C. Z., Bitew, M. A. (2021). Mobility-Aware Routing Algorithm for Mobile Ad Hoc Networks. Wireless Communications and Mobile Computing, 2021, 1–12. doi: https://doi.org/10.1155/2021/6672297
16. Zaki, S. M., Ngadi, M. A., Kamat, M., Razak, S. A. (2020). A Review of Location Prediction Techniques in Mobile Ad Hoc Networks. Al-Qadisiyah Journal Of Pure Science, 25 (2), 17–28. doi: https://doi.org/10.29350/qjps.2020.25.2.974
17. Haglan, H. M., Mostafa, S. A., Safar, N. Z. M., Mustapha, A., Saringatb, Mohd. Z., Alhakami, H., Alhakami, W. (2021). Analyzing the impact of the number of nodes on the performance of the routing protocols in manet environment. Bulletin of Electrical Engineering and Informatics, 10 (1), 434–440. doi: https://doi.org/10.11591/eei.v10i1.2516
18. Joy, A., Singh, K. (2017). Detection Mechanism for Jamming Attack in MANET. Int. J. Sci. Res. Dev., 4 (11), 604–607.
19. Fernendes, D., Rakesh Kumar, B. (2017). Survey on jamming attack in manet. International Journal of Latest Trends in Engineering and Technology, 410–414. Available at: https://www.ijltet.org/journal/151065846992.pdf
20. Hamdi, M. M., Audah, L., Abood, M. S., Rashid, S. A., Mustafa, A. S., Mahdi, H., Al-Hiti, A. S. (2021). A review on various security attacks in vehicular ad hoc networks. Bulletin of Electrical Engineering and Informatics, 10 (5), 2627–2635. doi: https://doi.org/10.11591/eei.v10i5.3127
21. Mahajan, A. S., Mahajan, S., Marwaha, M. (2017). Review of aodv & dsr protocols under jamming attack and recovery with pcf technique. Int. J. Softw. Hardw. Res. Eng., 5 (10), 14–17.
22. Xiao, X. (2008). Technical, Commercial and Regulatory Challenges of QoS. An Internet Service Model Perspective. Elsevier. doi: https://doi.org/10.1016/B978-0-12-373693-2.X0001-8
23. Kaler, V., Bairwa, A. K. et. al. (2017). Performance analysis of traffic oriented pcf in wireless local area network. International Conference On Communication & Computational Technologies, 312–318. Available at: https://ijcrt.org/papers/IJCRTICCC048.pdf
24. Jie, L., Wang, L. (2019). Simulation tools for MANETs: a systematic survey. International Journal of Advanced Trends in Computer Science and Engineering, 2 (11), 1045–1053. Available at: https://www.researchgate.net/publication/337949935_Simulation_tools_for_MANETs_a_systematic_survey
25. Nourildean, S. W., Mohammed, Y. A., Salih, A. M. (2022). Mobile Ad Hoc Network Improvement against Jammers for Video Applications Using Riverbed Modeler (v17.5). Webology, 19 (1), 1446–1459. doi: https://doi.org/10.14704/web/v19i1/web19096
26. Rao, Y. C., Kishore, P., Prasad, S. R. (2019). Riverbed Modeler Simulation-Based Performance Analysis of Routing Protocols in Mobile Ad Hoc Networks. International Journal of Recent Technology and Engineering (IJRTE), 7 (6S), 350–354. Available at: https://www.ijrte.org/wp-content/uploads/papers/v7i6s/F02690376S19.pdf