International Journal of Data and Network Science 7 (2023) 757–764

Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Simulation and analysis performance of ad-hoc routing protocols under DDoS attack and proposed solution

Ala Mughaid[a], Ibrahim Obaidat[a], Ashraf Aljammal[a], Shadi AlZu'bi[b], Fatima Quiam[b], Dena Abu Laila[a], Aseel Al-zou'bi[a] and Laith Abualigah[c,d,e*]

[a]*Department of Information Technology, Faculty of prince Al-Hussien bin Abdullah || for IT, The Hashemite University, PO Box 330127, Zarqa (13133), Jordan*
[b]*Computer Science Department, Faculty of Science and Information Technology, Al Zaytoonah University of Jordan, Amman, Jordan*
[c]*Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, Amman 19328, Jordan*
[d]*Faculty of Information Technology, Middle East University, Amman 11831, Jordan*
[e]*Applied science research center, Applied science private university, Amman 11931, Jordan*

C H R O N I C L E

Article history:
Received: December 2, 2022
Received in revised format: December 29, 2022
Accepted: February 5, 2023
Available online: February 5, 2023

Keywords:
Ad hoc networks
DSR
AODV
OLSR
Routing protocols
Wireless Networks and DDoS

A B S T R A C T

Ad hoc networks, known as infrastructure-less networks, are composed of mobile nodes that connect without a centralized system controlling them. These networks have a wide range of potential applications, including emergency response, events, military operations, wireless access, and intelligent transportation. They can take on various forms, such as wireless sensor networks, wireless mesh networks, and mobile ad hoc networks. Because users in these networks can move around at any time, routing protocols must adapt to the constantly changing network layout. However, these networks are also susceptible to various security threats, including DDoS attacks. This paper aims to analyze the performance and impact of security attacks on the performance of reactive and proactive routing protocols in CBR connection patterns with different pause times. The analysis is provided in metrics such as throughput, packet loss, end-to-end delay, and load. The simulation results show that, on average, the OPNET Modeler simulator analyzed the performance results under DDoS attacks under voice and video traffic conditions. Furthermore, the paper explores the use of Honeypot intelligent agents as a solution to increase security by creating a dummy node to fool DDoS attackers. The results show that the OLSR protocol is most affected by DDoS attacks in terms of quality-of-service metrics such as packet loss, throughput, end-to-end delay, and load. The number of responses to the honeypot solutions differs for each protocol.

1. Introduction

Ad hoc networks have received a lot of interest from the academic community in recent years due to the quick development of innovative new hardware such as smart mobile devices (Mughaid et al., 2022a), embedded platform software, Internet-of-vehicles, intelligent drones, and UAVs (Fratta et al., 2018.) Ad hoc networks are decentralized networks composed of mobile nodes with wireless hardware interfaces that enable wireless connections and allow packet generation and transmission. Since they don't require centralized management, these infrastructure-free networks support multi-hop groups on demand, extending wireless range (Saini & Sharma, 2019; Sharma, 2019). Ad hoc networks can be deployed rapidly to solve problems, making them useful for a variety of applications, including military applications (Usha, 2017), disaster area networks (Jahir et al.,

* Corresponding author.
E-mail address: aligah.2020@gmail.com (L. Abualigah)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2023.2.002

2019) and search and rescue operations (Anjum et al., 2017). They have also been used to link modern systems, such as the internet of things (IoT). Although research assumes the safety of ad-hoc routing algorithms, many ad-hoc network applications operate in unstable contexts. Most ad-hoc routing technologies are susceptible to a wide range of attacks, including DDoS attacks. The DDoS assault seeks to deplete the network's resources while preventing users from accessing services or using resources that are legitimately theirs by sending excessive, useless packets.

A distributed denial of service (DDoS) attack is any action that prevents a network from providing its intended services other than an attempt to destroy, disrupt, or impair the network (Marashdeh et al., 2021b; Mughaid et al., 2022c). DDoS assaults can happen at multiple layers in ad hoc networks. Jamming is one type of DDoS assault that can occur at the physical layer. Collision or interrogation attacks can happen at the connection layer. The network layer is susceptible to attacks like Black hole, HELLL flooding, and ICMP Ping Flood Attack. Attacks using SYN flooding are possible at the transport layer. Additionally, path-based DDoS assaults are a possibility at the application layer. This study suggests a technique for mimicking the ICMP Ping Flood Attack and investigating how it affects wireless routing technologies using the OPNET Modeler tool.

Based on how they function, wireless network routing techniques can be categorized into two groups: proactive and reactive. Ad-hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are two examples of reactive routing protocols that have the benefit of being flexible to network changes and obviating the need for routine updates. They also suffer from high flood-search overhead and mobility issues, which is a drawback. Conversely, proactive routing protocols employ conventional distributed shortest-path strategies and demand frequent updates, resulting in increased routing overhead. The Optimized Link State Routing Protocol is one example of a proactive routing protocol (OLSR).

• Created in 2007, Dynamic Source Routing (DSR) is a self-organizing and self-configuring routing technology for wireless networks. It has components for route discovery and route maintenance, which jointly determine the most effective way for transmission between a source and a destination and modify the path in response to changing network conditions.

• Ad-hoc Developed in 2003, On-demand Distance Vector (AODV) Routing is a unicast routing protocol that chooses paths to destinations within the ad hoc network with a little burden on the processor and memory, as well as with little network consumption.

• The Optimized Link State Routing Protocol (OLSR) was created in 2014 and is a proactive, table-driven protocol. To share topological data, it frequently communicates with other network nodes. For effective routing, each node chooses a set of its neighbors to serve as "multipoint relays" (MPRs).

During a ping flood, a target device is subjected to a denial-of-service attack that aims to overwhelm it with ICMP echo-request packets and make it inaccessible for regular traffic. A DDoS attack, also known as a distributed denial-of-service attack, is one in which the attack traffic originates from several devices and is defined by the attackers' deliberate attempt to block authorized users from using a service. In this study, we analyze how this assault affects each protocol's service quality and investigate ways to strengthen network security and lessen DDoS attacks.

Distributed denial-of-service (DDoS) attacks are a significant threat to ad hoc networks. Attackers continually modify their tools to compromise security systems, while researchers modify their tactics to deal with new threats. The DDoS field is rapidly growing more complex, and several defense measures to address the problem have been presented.

The general objective of this paper is introduced as follows:

- Acquire a basic comprehension of ad hoc networks.
- Simulate and analyze the performance of three types of Ad-hoc network routing protocols before and after a DDoS assault.
- Investigate ways to improve the security of these networks and mitigate DDoS attacks.

Following is how the remaining sections of the essay are structured: Some older works are displayed in Section 2. Section 4 describes and analyzes simulation results before and after the DDoS attack and describes a proposed technique that attempts to lessen the impact of the DDoS attack on the performance and security of ad hoc networks and its outcome. Section 3 Methodology describes the simulation setup and performance metrics. Section 5 brings us to a close.

2. Lecture Review

The three conventional methods of network queue management are drop-tail, RED, and REM. The effectiveness of these techniques was assessed in terms of packet rate and average end-to-end delay under DDoS attacks, according to the study by Mirkovic (2004), which used the network simulation program NS2. The findings demonstrated that active queue management algorithms, such as REM and RED, outperformed Drop-Tail's passive queue management technique in thwarting medium- and small-scale DDoS attacks. All three methods, however, were discovered to be insufficient for fending off significant DDoS assaults.

In addition to a well-known attack, the Black Hole attack, they looked into a novel DoS attack used by Jellyfish: relay nodes that covertly misorder, delay, or drop packets that they are supposed to forward, causing end-to-end congestion management measures to fail (Aad et al., 2008). They investigated these attacks in several circumstances and calculated the damage they could cause. They used a basic analytical model and many simulation experiments to examine the effects of various performance aspects and provide a quantitative evaluation of how DoS attacks affect performance and scale in ad hoc networks.

Reddy and Thilagam (2020) used NS2 to test the network's performance by implementing DDoS attacks, non-attack, and DDoS attacks with recommended method simulation scenarios. According to their simulation results, their recommended solution reduces the severity of DDoS attacks while processing eighty percent of the legal traffic. However, without their suggested method, network nodes in a hostile environment only process 0% of genuine traffic.

Reddy and Thilagam (2020) discussed DDoS assaults in wireless ad hoc networks and developed a defense method to mitigate the attack. They use rate-limiting to stop malicious network flows and precisely identify DDoS attack flows. Their recommended security strategy successfully identifies the attackers; once they are identified, the attack traffic is deleted, enabling regular users to access network resources. They contrasted the effectiveness of their suggested plan with the SWAN plan. Simulation findings showed that their suggested approach offers improved performance, providing legitimate users with larger bandwidth received, a higher packet delivery ratio, and a lower packet drop rate.

A path-based method for recognizing black-hole and other sorts of assaults was provided in a research by (Arunmozhi & Venkataramani, 2011). The authors created an adaptive algorithm to enhance this method's detection performance after carefully weighing its advantages and disadvantages. The simulation's outcomes demonstrated that attacks with a gray magnitude of more than 60% can seriously damage the network. They also contrasted their approach with others and discovered that it significantly enhances detection. A lower detection rate but a lower false positive rate adaptive detection technique was also investigated for its trade-offs in the study.

According to the investigation in 2010 (Cai et al., 2010), the rushing attack is a novel and successful defense against ad hoc network routing systems. Additionally, a ground-breaking mechanism known as RAP (Rushing Attack Prevention), which protects against rushing attacks, was put into place. With this method, any secure on-demand ad hoc network routing system that has previously been proposed is vulnerable to a denial-of-service attack.

3. Simulation Setup and Performance Metrics

OPNET modeler v14.5 was utilized as a simulation tool to implement these experiments, as shown in Fig.1.The simulation setup of nine scenarios analyzed quantitative evaluation of routing protocols and applied DDOS attack using OPNET simulator. By examining how routing protocols affect the amount of data delivered through a wireless network while it is not under attack, when it is under attack, and when mitigation measures are used, this experiment tries to assess the effectiveness of routing protocols. We have evaluated the performance of three well-known routing protocols, OLSR, AODV, and DSR, for the following performance metrics: throughput, packet loss, end-to-end delay, and load, under the simulated configuration shown in Table 1.

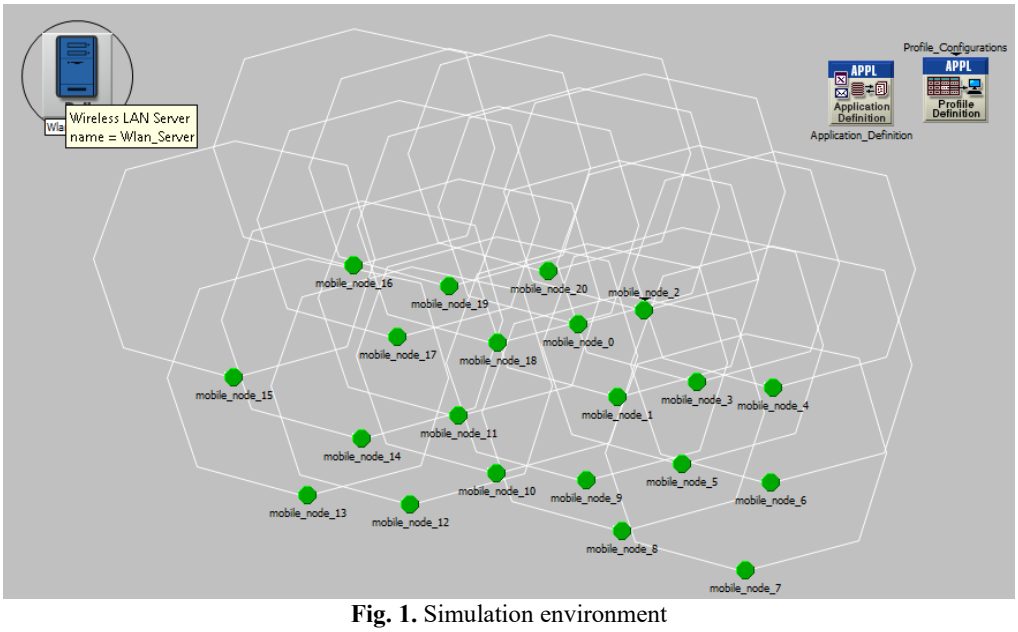

Fig. 1. Simulation environment

Table 1
Simulation Parameters

Parameters	Values	Parameters	Values
Number of nodes	22	Protocols	AODV, DSR, OLSR
Data Rate (Bandwidth)	11mbps	MAC Protocol	802.11
Packet size	exponential(1024)	Simulation Time	600s
Mobility Speed	1-15m/s	Mobility Model	10 m/sec
Scenario Size	100m × 100m	Attack Type	DDOS
Power Threshold(dBm)	-95	Transmit power(w)	0.005

3.1 Performance Metrics

- Packet Drop/Loss: The total number of packets that are dropped from a network due to a connection loss or network congestion is referred to as packet drop/loss. It is calculated by dividing the difference between the number of sent packets and the number of received packets by the number of sent packets as follows:

  DP= (nSentPackets- nReceivedPackets)/ nSentPackets
  where nReceivedPackets = Number of received packets, nSentPackets = Number of sent packets

- Throughput: It is a measure of the amount of data that is successfully transmitted over a given period. It is calculated by dividing the total number of packets received across all destinations by the transmission duration and measured in Kbps.

- End-to-end delay: It is the total amount of time it takes for a packet to reach its destination. It is measured in milliseconds and calculated by taking the sum of the difference between the reception time and the send time for all packets successfully delivered and dividing by the number of packets as follows.

$$D = \frac{1}{n}\sum_{i=1}^{n}\left(Tr_i - Ts_i\right)\times 1000\left[ms\right] \tag{1}$$

  where D = Average E2E Delay, i = packet identifier, Tr_i = Reception time, Ts_i = Send time, n = Number of packets successfully delivered.

- Load: It is a measure of the amount of data (traffic) that the network is carrying at a given time. It is often represented as a percentage of the network's maximum capacity.

4. Simulation Results and Discussion

In three different scenarios—(a) normal operation, (b) under a DDoS attack, and (c) after implementing the suggested mitigation technique—we evaluated and compared the performance of well-known Ad-hoc network routing algorithms using tables and graphs for each of the performance metrics as described below. In order to implement our suggested method, we used a network simulator (OPNET). We built nine scenarios with 22 network nodes, of which 20 nodes showed typical behavior and two nodes showed DDoS attack behavior. In order to create the 655527 DDoS attack traffic depicted in Fig. 2, we employed Constant Bit Rate (CBR) traffic with a packet size of 1024 bytes for regular traffic and 1000 bytes for aberrant activity.

Numerous methods try to lessen the impact of DDoS assaults on the functionality and security of ad hoc networks. In this section, a honeypot application was suggested. A honeypot is an attack trap that records the activity of the attack source while simulating some or all of a real system's behavior (Sardana, 2011; Hu et al., 2003). On the server side, honeypots can be utilized in a variety of ways to not only detect DDoS attacks but also to secure user-sensitive data and report any malicious activity so that the attacker can be found (Deshpande, 2015).

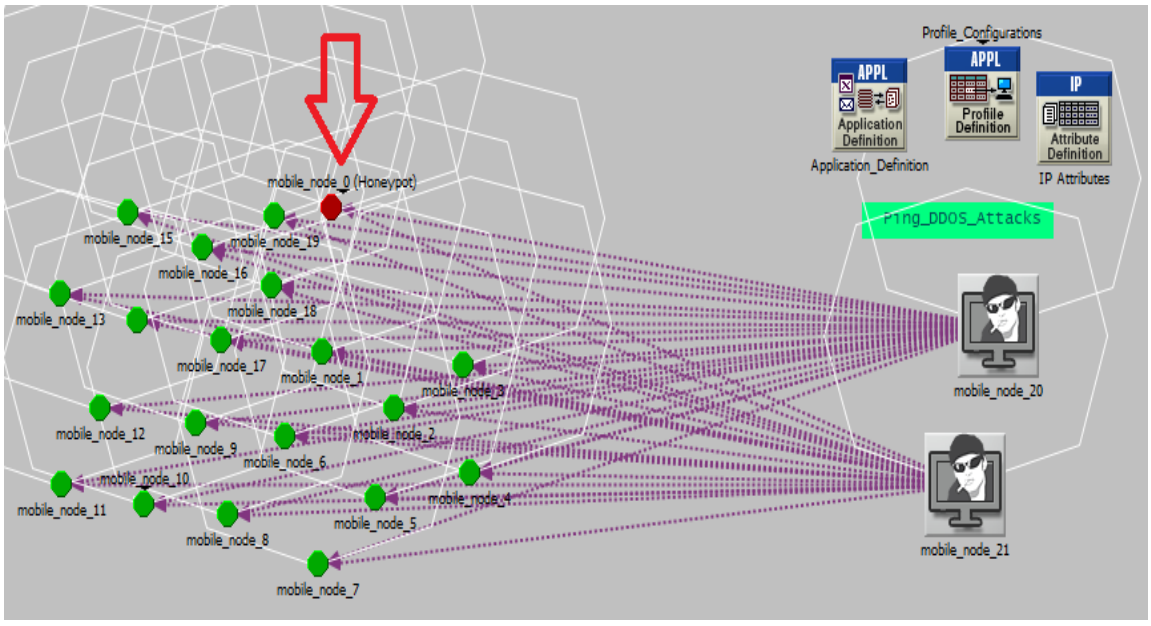

Fig. 2. Honeypot Simulation.

4.1 performance metric

In this section, we will discuss four performance matrices with three of the protocols, each separately, and each protocol with three scenarios (without attack, with attack, and after mitigation).

4.1.1 Packet Loss/Drop Packet

The first performance metric is Drop Packet ;as shown in Table 2, there was no loss in the packet before an attack, unlike under attack, the number increased significantly. Still, with the application of the mitigation tool, the value returned to 0 in the AODV protocol, while OLSR decreased the value a lot, while DSR decreased, but slightly. These findings show that a total amount of higher layer data traffic (measured in bits/sec) was dropped by all WLAN MACs in the network due to repeatedly unsuccessful retransmissions. These packets were identified in later Block-ACKs and deleted since the transmit lifetime limit had been surpassed because the MAC did not receive any ACKs for those packets' (re)transmissions. We should also highlight that the AODV protocol has the fewest drop packets due to the nature of its operation, which requires the node to register only the next node rather than all paths in the database to discover the proper path.

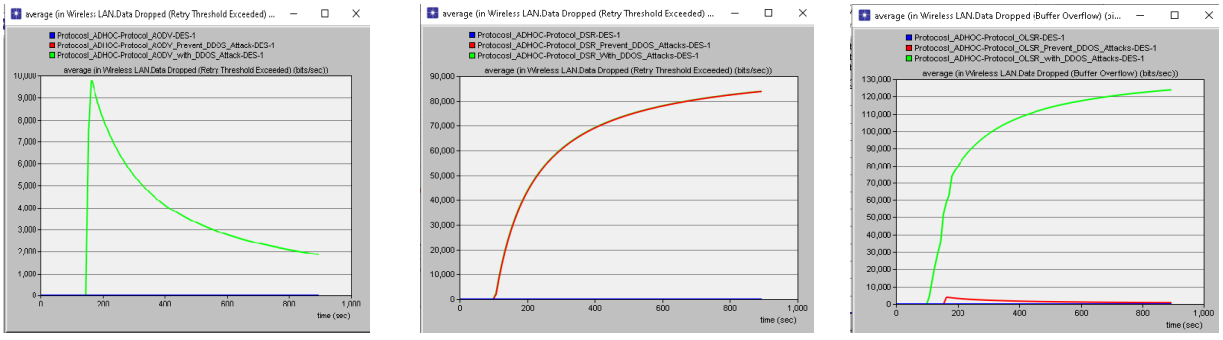

Fig. 3. Packet Loss/Drop Packet for each protocol in different scenario

Table 2
Packet Loss/Drop Packet for each protocol in different scenarios

	AODV	DSR	OLSR
Without attack	0	0	0
Under attack	323131.6	5920161	9144844
After mitigate	0	5902382	125092.6

4.1.2 Throughput

The second performance parameter is throughput, The total number of bits (in bits/sec) transported from a lower layer of wireless LAN to a higher layer in all network WLAN nodes. Table 3 shows that the number of packets transmitted without an attack is significantly lower than that of packets sent with an attack. If we compare the number of packets in each protocol, we notice that the OLSR protocol contains the most significant number because the protocol is proactive and works immediately by sending broadcasts to other nodes; it is affected the most in throughput, While the DSR protocol is the least affected because it stores only ten hops on its table. When we apply our tool to these protocols, the numbers are significantly reduced because we hid the network, which became hidden from the attacker.

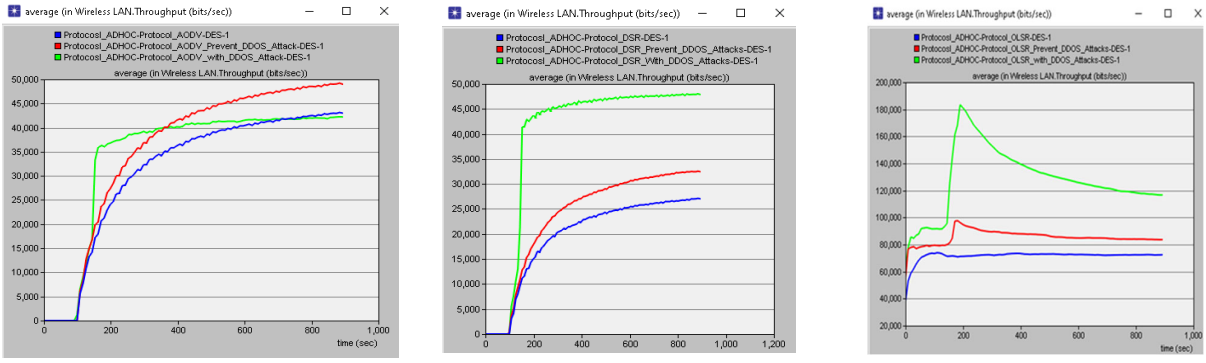

Fig. 4. Throughput for each protocol in different scenarios

Table 3
Throughput for each protocol in different scenarios

	AODV	DSR	OLSR
Without attack	3108832	1947044	7157228
Under attack	3416399	3914667	12741628
After mitigate	3551040	2339708	8529516

4.1.3 End-to-End Delay

Each packet that is received by the wireless LAN MACs of every WLAN node in the network and transmitted to the upper layer experiences an end-to-end delay. As we can see in the normal mode without attack, the OLSR (proactive protocol) protocol has the most delay value. In the attack mode, it also has the most significant value because it works continuously to update the table. In contrast, AODV and DSR (reactive protocols) have the lowest value. DSR is less than OLSR because DSR contains TTL, while OLSR does not contain TTL, and the values remain in the table until another request comes from the node, and we will be able to overcome this delay in the proposed method as we note its effectiveness in Table 4.

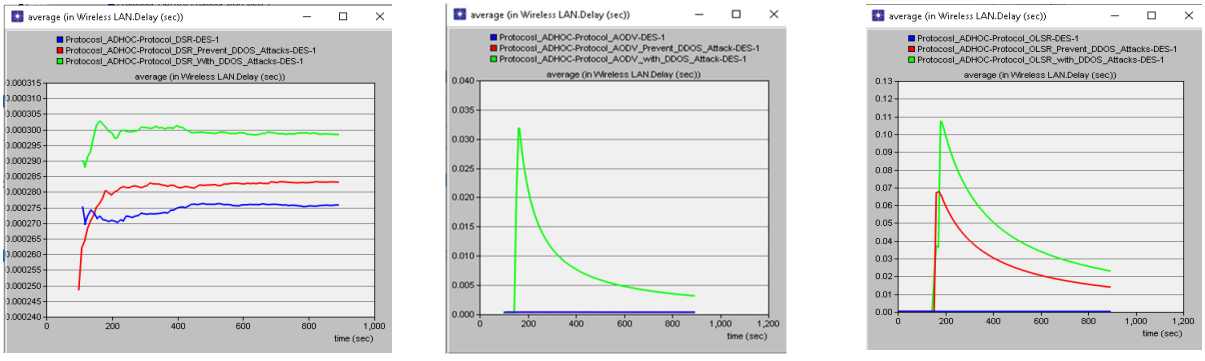

Fig. 5. End-to-End delay for each protocol in different scenarios

Table 4
End-to-End delay for each protocol in different scenarios

	AODV	DSR	OLSR
Without attack	0.031076	0.024158	0.026343
Under attack	0.676233	0.026303	3.743324
After mitigate	0.031688	0.025002	2.341088

4.1.4 Load

The last performance indicator, load, measures the total amount of data (in bits/sec) that all WLAN nodes in the network's upper tiers send to the wireless LAN layers. As we note in a protocol OLSR that contains the most significant value in the three scenarios, the reason is that it always works on a continuous update of the table, representing a load on the network. At the same time, AODV and DSR contain similar values but much less than OLSR.

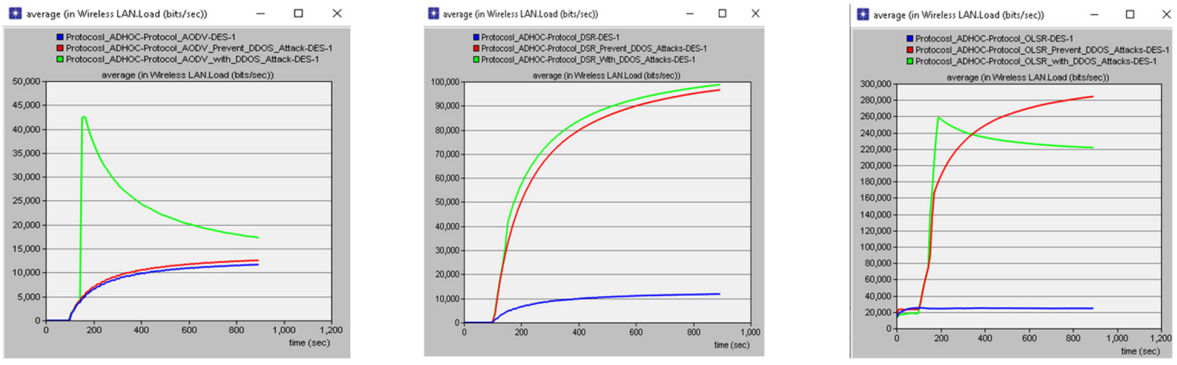

Fig. 6. Load for each protocol in different scenarios

Table 5
Load for each protocol in different scenarios

	AODV	DSR	OLSR
Without attack	840092.3	848689.7	2425397
Under attack	1991836	7142350	19523497
After mitigate	902635.5	6820579	21345771

4.2 The comparison of the proposed method with the related methods

Table 6 demonstrates the similarities and differences between the proposed method of this paper and other studies.

Table 6
The proposed method versus other methods

Study	Study methodology	The proposed method
(Wei et al., 2017)	In order to fend off DDoS attacks, the authors of the research experimented with using three conventional network queue management techniques, namely Drop-Tail, RED, and REM.	Three different types of conventional network protocols—AODV, DSR, and OLSR—were subjected to DDOS attacks on ad-hoc routing protocols environments.
(Aad et al., 2008)	They provide a quantitative assessment of how DoS assaults affect performance and scale in ad hoc networks.	Denial of Service (DoS) assaults on ad hoc networks are assessed mathematically and qualitatively in our study, along with their impacts and scalability.
(Reddy & Thilagam, 2020)	To identify DDoS attack traffic patterns, they employ a unique network node authentication module and naive Bayes classifier module.	We prevent the DDoS attack by hide the BSS identifier of the network.
(Arunmozhi & Venkataramani, 2011)	They recommended discarding the assault traffic once the attackers were identified.	We suggested defense method by hide the BSS identifier of the network from the attacker to prevent the DDoS attack.
(Cai et al., 2010)	They used the DSR protocol for their algorithm and applied it to ns-2 and the average detection rate was above 90%	We used three protocol and apply it on OPNET simulator, The mitigation average is up to 99% for some protocols.
(Hu et al., 2003)	The authors evaluated RAP against on-demand ad-hoc network routing protocols and presented RAP (Rushing Attack Prevention), a new approuch that defends against rushing attacks.	We conducted an evaluated RAP against on-demand ad-hoc network routing protocols and presented RAP (Rushing Attack Prevention), a new protocol that defends against rushing attacks.

5. Conclusion

Under this study, we used the OPNET simulator to evaluate the effectiveness of three AD-Hoc network routing protocols (DSR, AODV, and OLSR) in diverse circumstances. The first scenario depicts business as usual, the second depicts a DDoS attack, as well as the third depicts business as usual with the suggested mitigation approach. To examine the data, we employed parameters including throughput, packet loss, end-to-end delay, and load. In order to improve the security of these networks, we also investigated the usage of Honeypot intelligent agents, which are virtual software agents that imitate a dummy node to fool DDOS attackers. According to the findings, OLSR was the protocol that was most negatively impacted by a DDoS

attack in terms of packet loss, throughput, end-to-end delay, and load. How well the honeypot solutions work to mitigate the attack on each protocol varies.

References

Aad, I., Hubaux, J. P., & Knightly, E. W. (2008). Impact of denial of service attacks on ad hoc networks. *IEEE/ACM transactions on networking, 16*(4), 791-802.

Anjum, S. S., Noor, R. M., & Anisi, M. H. (2017). Review on MANET based communication for search and rescue operations. *Wireless personal communications*, *94*(1), 31-52.

Arunmozhi, S. A., & Venkataramani, Y. (2011). Ddos attack and defense scheme in wireless ad hoc networks. *arXiv preprint arXiv:1106.1287*.

Cai, J., Yi, P., Chen, J., Wang, Z., & Liu, N. (2010, April). An adaptive approach to detecting black and gray hole attacks in ad hoc network. In *2010 24th IEEE international conference on advanced information networking and applications* (pp. 775-780). IEEE.

Fratta, L., Gerla, M., & Lim, K. W. (2018). Emerging trends and applications in ad hoc networks. *Annals of Telecommunications*, *73*, 547-548.

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

Jahir, Y., Atiquzzaman, M., Refai, H., Paranjothi, A., & LoPresti, P. G. (2019). Routing protocols and architecture for disaster area network: A survey. *Ad Hoc Networks*, *82*, 1-14.

Marashdeh, Z., Suwais, K., & Alia, M. (2021, July). A survey on sql injection attack: Detection and challenges. In *2021 International Conference on Information Technology (ICIT)* (pp. 957-962). IEEE.

Mughaid, A., Al-Zu'bi, S., Al Arjan, A., Al-Amrat, R., Alajmi, R., Zitar, R. A., & Abualigah, L. (2022a). An intelligent cybersecurity system for detecting fake news in social media websites. *Soft Computing*, *26*(12), 5577-5591.

Mughaid, A., AlZu'bi, S., Alnajjar, A., AbuElsoud, E., Salhi, S. E., Igried, B., & Abualigah, L. (2022b). Improved dropping attacks detecting system in 5g networks using machine learning and deep learning approaches. *Multimedia Tools and Applications*, 1-23.

Mughaid, A., AlZu'bi, S., Hnaif, A., Taamneh, S., Alnajjar, A., & Elsoud, E. A. (2022c). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*, *25*(6), 3819-3828.

Reddy, K. G., & Thilagam, P. S. (2020). Naïve Bayes classifier to mitigate the DDoS attacks severity in ad-hoc networks. *International Journal of Communication Networks and Information Security*, *12*(2), 221-226.

Saini, T. K., & Sharma, S. C. (2019). Prominent unicast routing protocols for Mobile Ad hoc Networks: Criterion, classification, and key attributes. *Ad Hoc Networks*, *89*, 58-77.

Usha, R., Premananda, B. S., & Reddy, K. V. (2017, June). Performance analysis of MANET routing protocols for military applications. In *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1063-1068). IEEE.

Wei, W., Song, H., Wang, H., & Fan, X. (2017). Research and simulation of queue management algorithms in ad hoc networks under DDoS attack. *Ieee Access*, *5*, 27810-27817.