Wormhole Attack Vulnerability Assessment of MANETs: Effects on Routing Protocols and Network Performance

Ferdinand Alifo
MIS/Computer Dep., Ministry of Local Government, Local Gov't Service. Kumasi, Ghana

Doe Martin
Information Techology Department
Valley View University
Accra, Ghana

Mustapha Awinsongya Yakubu
University of Cincinnati Ohio, USA

ABSTRACT

This paper discusses Mobile Ad-hoc Networks (MANETs), which are self-organizing networks without infrastructure relying on wireless connections between mobile nodes. The open communication channels in MANETs make them vulnerable to attacks, compromise privacy, and reduce throughput. The paper aims to investigate the impact of wormhole attacks on MANETs, highlighting the significant security threat they pose to wireless networks despite the presence of authentication and confidentiality measures. This paper utilized ns-allinone-2.35-RC7 as a simulation environment to study the effects of introducing wormhole nodes into the network. The DSDV and TORA routing protocols were significantly impacted by wormhole attacks, leading to limited data transmission and a low packet delivery ratio. Conversely, the DSR protocol performed better, demonstrating higher average throughput, successful data transmission, and improved resistance against wormhole attacks.

General Terms

Wormhole attacks significantly impact DSDV and TORA routing protocols in Mobile Ad-hoc Networks, despite authentication measures, while the DSR protocol exhibits greater performance.

Keywords

Security, Performance, Analysis MANET, TORA, DSR DSDV, Attack, Wormhole

1. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) give considerable importance to routing protocols, making it an intriguing and demanding area of investigation. Several routing protocols, such as AODV, DSR, DSDV, TORA, and others, have been specifically designed to address the distinctive needs of MANETs. Ensuring secure routing operations is of utmost significance to ensure the effective performance of MANETs, which are vulnerable to attacks due to factors like open access, dynamic network topology, lack of central administration, cooperative algorithms, and limited protective mechanisms [1]. Addressing security issues is crucial to ensure data reliability, user privacy, and network service availability. Potential challenges include saturating assaults, routing table overflow attacks, DoS attacks, Sybil attacks, wormhole attacks, and impersonation attacks [2]. A comprehensive exploration of MANETs' behavioural characteristics is crucial for enhancing security and protecting user privacy. Security is of utmost importance in Mobile ad-hoc network protocols due to their susceptibility to numerous security threats, with Wormhole attacks being prevalent. Analyzing the performance of two reactive and one proactive (TORA, DSR, and DSDV) MANET protocols under wormhole attacks can offer valuable insights into the vulnerabilities of these MANET [3]. Among the most severe attacks in MANETs is the Wormhole Attack, which drops packets in the network when access is gained [4]. A wormhole attack disrupts MANETs by circumventing established protocols by creating a shortcut tunnel that deceives protocols into recognising the wormhole as a reliable route. The entire network's functioning could be interfered with by this malicious attack, which would negatively impact the quality of service offered [5]. The Wormhole Attack poses a substantial risk to MANETs and is considered one of the most dangerous attacks. It has been observed to affect MANET protocols such as AODV, DSR, DSDV, and TORA. Hence, it is crucial to prioritise network security to improve the availability of network services and safeguard user privacy [6].

2. RELATED WORKS

Ad hoc networks are temporal networks that form on request without the use of an existing infrastructure. Ad Hoc Networks are used in a variety of contexts, including business, industry, and social situations, to guarantee Quality of Service (QoS), according to [7]. These networks also prove valuable in emergency situations like disaster recovery. Due to their dynamic nature, ad-hoc networks are well-suited for internetworking applications where new networks are frequently established.

An ad hoc network is created spontaneously as devices establish connections and communicate with one another. The term "ad hoc," originating from Latin, conveys the idea of being purposefully formed for immediate use [8]. This network type offers significant benefits by enabling the quick establishment of device-to-device connections without the need for pre-existing infrastructure. In a decentralized arrangement by the Ad-Hoc Network, every device actively engages in the routing process by employing a routing algorithm to select an appropriate path. Data is then transmitted to other devices along the chosen path, facilitating efficient communication within the network [8].

2.1 Types of MANETs

According to [13], a Mobile Ad-hoc Network (MANET) is a dynamic network made up of mobile devices that can connect to one another over wireless networks. Notably, MANETs do not require a fixed infrastructure or centralised administration for operation. In a MANET, the network nodes possess the capability to communicate directly with one another, eliminating the dependency on a central access point or base station. This decentralised nature enables the nodes to self-configure and establish ad-hoc connections, making MANETs highly flexible and adaptable for various scenarios.

2.1.1 Smart Phone Ad-Hoc Network (SPANS)

These Ad-hoc Networks demonstrate the potential of cell phones. Ad hoc smartphone networks allow for direct phone-to-phone communication by utilising accurate neighbourhood and path detection techniques. Unlike older connection techniques such as hub and spoke networks, ad hoc networks are decentralised and support multi-hop routing, allowing devices to enter and exit the network as needed. Direct device communication is made possible in ad hoc networks by the lack of a need to assign a leader or peer [9].

2.1.2 Internet Based Mobile Ad Hoc Network (IMANET)

Utilising MANET technology allows for the self-organisation of mobile networking infrastructures. This innovation enables a network of mobile nodes to establish autonomous connectivity to the Internet. In the digital domain, this technology effortlessly accommodates protocols like Transmission Control Protocol (TCP) on top of User Datagram Protocol (UDP) or Internet Protocol (IP). These protocols are essential in enabling the connection of mobile nodes and establishing distributed and ad hoc routes for effective communication within the network.

2.1.3 Vehicular Ad Hoc Network (VANET)

Integration of vehicle-to-vehicle and vehicle-to-roadside architectures inside a Vehicular Ad Hoc form has been identified as a strategy to improve highway safety, navigation, and other roadside services. In the context of intelligent transportation systems, VANETs serve as a vital component, gradually evolving into a comprehensive "car internet" and potentially evolving further into an "autonomous vehicle internet." This interconnected "car internet" enables seamless communication among vehicles, both on and off the road, creating a dynamic network for efficient information exchange [10].

2.1.4 Military or tactical Mobile Ad hoc Networks (MANETs)

Military or tactical Mobile Ad hoc Networks (MANETs) are utilised by military units with a primary emphasis on quick mobilisation, infrastructure-free communication, and reliance on wireless connectivity rather than fixed radio towers. Networks (MANETs) are utilized by military units with a primary emphasis on quick mobilization. These networks are meant to be durable and are widely used in cases when soldiers need to communicate in remote or foreign lands while moving or evading potential impediments, also known as "hopping" or "leapfrogging" army mines. This type of network is also known as an "on-the-fly" tactical wireless network, as described by [11].

2.1.5 Flying Ad hoc Networks (FANET)

FANETs have undergone recent changes due to the advancement and extensive utilisation of Unmanned Aerial Vehicles (UAVs), such as drones and satellites. Only aerial devices can communicate with each other and with ground-based UAV-to-ground devices in networks called FANETs. Small drones and tiny drones can be categorised as high- and medium-range UAVs based on UAVs built from small drones [12].

2.2 Types of MANETs Routing Protocols

In the realm of Mobile Ad hoc Networks (MANETs), there are two significant types of routing protocols: reactive (on-demand routing) and proactive (table-driven) protocols. Additionally, a hybrid routing protocol that integrates both proactive and reactive routing approaches exists as another illustration of the fundamental routing protocols utilised in MANETs, as highlighted by [14] Showed in figure 1.

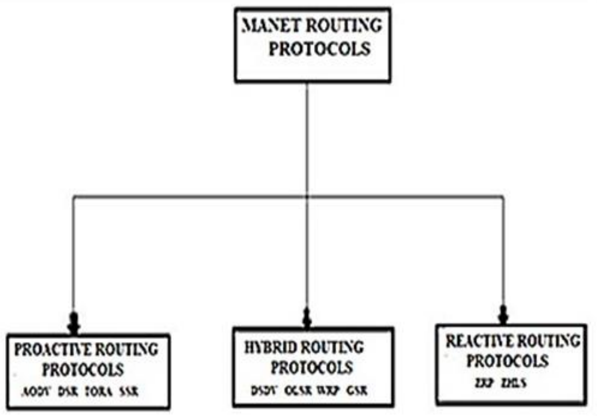


Fig.1. Classification of MANET Routing protocols

2.2.1 Reactive routing protocols

According to a study by [15], reactive routing protocols are known as on-demand protocols when the routing paths are known. The method used to determine a route is known as route determination. This method is repeated until either the best route has not been found or all feasible route permutations have been crossed. Unlike proactive routing protocols, reactive protocols only establish routes when they are specifically requested, leading to lower overhead in route management, which essentially becomes their advantage.

The AODV, TORA, and DSR routing protocols are well-known reactive routing protocols designed to establish pre-determined paths for information packet transmission. Unlike proactive protocols, these protocols do not involve proactive information exchange between nodes or neighbouring nodes in the network. Instead, once the packets are forwarded to them, nodes maintain the established route to the destination. This approach, as described in the study by [15], promotes efficiency in the routing process and enables effective packet delivery within the network.

2.2.2 Proactive Routing Protocols

Proactive routing protocols, according to [16], are table-driven since any other devices in the network setup keep a routing table, including details about the network's topology and any available adjacent nodes. A source node uses extremely reliable routing tables to locate a target node within the network whenever it has to deliver a datagram to a destination node. If the network topology changes, a transmission message is sent to every node in the network to update the routing table. Several advantageous MANET routing strategies inherit wired network routing algorithms with few adjustments. Regardless of the data or traffic being transmitted, nodes can change routing information using these protocols. With some essential modifications, several beneficial MANET routing techniques inherit wired network routing algorithms. Nodes can change routing information using these protocols, regardless of the data or traffic being transmitted.

The Bellman-Ford method and the Order of Arrival were used to create this protocol, which employs vectors, an example and the most widely used is the DSDV protocol [17]. This protocol maintains all of the node's information. All mobile nodes are required to broadcast their entries to nearby nodes. After mutual consent, the nodes along the path send the data packet from one to the next. To prevent a route interruption, each node must maintain accurate information about their location in the tables at all times.

2.2.3 Hybrid Routing Protocol

Routing protocols that include proactive and reactive elements are called hybrid routing protocols [18]. Hybrid routing protocols are intended to lower latency in reactive routing protocols while simultaneously reducing the control overhead brought on by proactive routing techniques. Hybrid routing technologies typically have topologies that are zone- or region-based. Typically, a table-driven protocol is used for data transmission inside the region (proactive). When data transmission between multiple regions or zones is required, on-demand routing techniques are used.

The commonly employed hybrid routing protocols encompass Zone Routing Protocol (ZRP), Fisheye State Routing (FSR), Landmark Ad hoc Routing (LANMAR), Relative Distance Micro-Discovery Ad hoc Routing (RDMAR), and Scalable Location Update-based Routing Protocol (SLURP).

Table 1. Comparison of Proactive, Reactive and Hybrid Routing Protocols

Parameter	**Proactive routing Protocols**	**Reactive routing Protocols**	**Hybrid routing Protocols**
Routing Scheme	Table driven routing	On-demand routing	Mixture of Proactive and Reactive
Overhead	High Routing Overhead	The routing overhead is low	Medium Routing Overhead
Scalability	Low scalability	Not suitable for larger network	Suitable for larger Networks
Traffic	High	Low	High inside the zone and low outside the zone
Latency	Low	High because of flooding	Latency is low inside the zone and is high outside

3. PORPOSED MODELLING

In this paper, NS-2 was selected as it is one of the most popular network simulation packages for studies in wireless networks [19]. The research design was divided into five sections: simulator installation, protocol selection, simulation parameter settings, selection of performance metrics, and analysis.

3.1 Simulation Installation and Protocol Selection

Cygwin was selected, which is a Linux-like environment designed for Windows operating systems, providing essential tools and libraries for NS-2, a discrete event simulator for network research and simulation. Cygwin can integrate NS-2 with Windows by downloading and installing the NS-2 ns-allinone-2.35-RC7 package, which includes NS-2 and its dependencies. This integration allowed us to use NS-2 for simulating and analysing network scenarios while using the Windows operating system's Linux-like environment. The NS-2 ns-allinone-2.35-RC7 package compatible with Cygwin was downloaded and installed from the NS-2 website.

Two Reactive Routing Protocols (DSR and TORA) and one Proactive Routing Protocol (DSDV) were selected for the experiment.

DSR, a reactive routing protocol, was also selected, which is designed for ad-hoc networks to reduce control packet bandwidth consumption (IETF MANET draft RFC 4728, 2007). DSDV is a proactive protocol using Bellman-Ford algorithms [20], while TORA is an on-demand protocol initiated by the source node to minimize communication overhead. These protocols offer scalability, efficiency, and avoid loops while also utilizing the link reversal algorithm.

3.2 Simulation Parameters

Simulation parameters govern system dynamics, influencing outcomes through numerical values, probabilities, and capacities.

Table 2 Simulation parameters

Parameter	**Settings**
Channel type	Wireless channel
Radio-propagation model	Two Ray Ground
Network interface type	Wireless Phy
MAC type	802.11
Interface queue type	Queue/DropTail/PriQueue,MUPriQueue
Simulation time	10 seconds
Topography dimension	1440 by 100
Link layer type	LL
Antenna model	Omni Antenna
Max. packet in queue	50
Number of mobile nodes	16
Routing protocol	DSDV, DSR, TORA
Number of wormholes	2

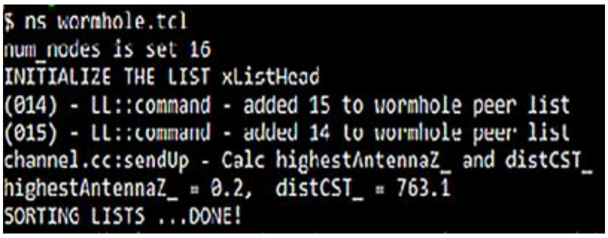
3.3 Performance Metrics

The paper focuses on three performance metrics: average throughput, average delay, and packet delivery ratio. Average throughput measures the speed at which data is successfully transferred or processed, indicating a system's efficiency in managing data. The packet delivery ratio determines the successful delivery of packets to their intended destination, with a higher ratio indicating a more reliable network with minimal packet loss. The average packet delay represents the average time it takes for a packet to traverse from a source node to a destination node within a network.

3.4 Simulation Experiment

The NS-2 test-bed was used for simulation experiments, and four files were run on the simulator. Tcl files contain configuration files for node creation, network topology creation, link setup, and protocol configuration. Awk files were created for processing trace files generated by NS-2 simulators. The study used AWK files to calculate performance parameters such as average throughput, packet delivery ratio, and average delay. The location path for the files was C:/cygwin/home/Noureddinens-allinone-2.35-RC7/ns-2.35/worm. The path of the three key files required for NS-2 to run was set in the.bashrc file. Simulation Experiment

Interface queue type was set to Queue/DropTail/PriQueue, Routing protocol was set to DSDV, trace file was set to [open dsdv.tr w], nam file was set [open dsdv.nam w], node 12 was set as source node at initial position X-axis =299 : Y-axis =400, node 13 was set as destination node at initial position X-axis = 900 : Y-axis = 399, node 14 was set as wormhole node at position X-axis = 300 : Y-axis = 500 and node 15 was set as wormhole node at position X-axis = 900 : Y-axis = 300 with initial output shown in fig 2.

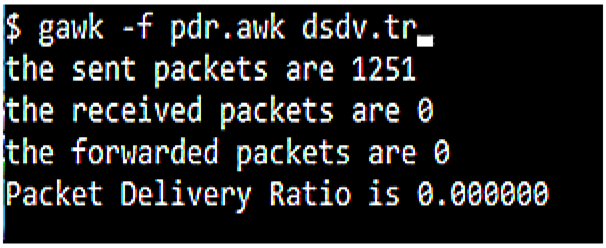


```
$ ns wormhole.tcl
num_nodes is set 16
INITIALIZE THE LIST xListHead
(014) - LL::command - added 15 to wormhole peer list
(015) - LL::command - added 14 to wormhole peer list
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 0.2,  distCST_ = 763.1
SORTING LISTS ...DONE!
```

Fig: 2. Output of wormhole.tcl file execution for DSDV

3.4.1 Simulation Experiment and Output for DSDV

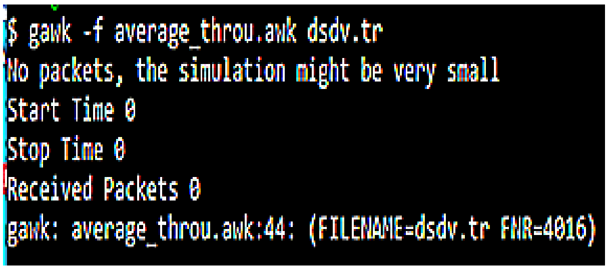
Packet Delivery ratio was executed with gawk –f pdr.awk dsdv.tr command resulted in an output shown in fig 3.



```
$ gawk -f pdr.awk dsdv.tr
the sent packets are 1251
the received packets are 0
the forwarded packets are 0
Packet Delivery Ratio is 0.000000
```

Fig: 3 Packet delivery ratio for DSDV

Average throughput for DSDV was executed with gawk –f average_throughput.awk dsdv.tr command resulted in an output shown in Fig. 4.



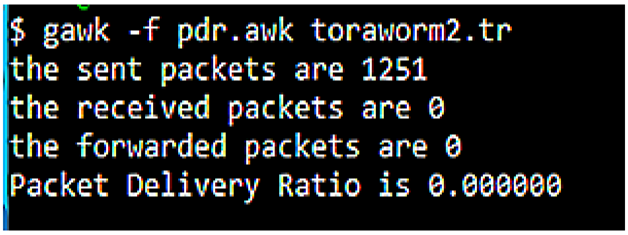
```
$ gawk -f average_throu.awk dsdv.tr
No packets, the simulation might be very small
Start Time 0
Stop Time 0
Received Packets 0
gawk: average_throu.awk:44: (FILENAME=dsdv.tr FNR=4016)
```

Fig: 4 Average Throughput for DSDV

3.4.2 Simulation Experiment and Output for TORA

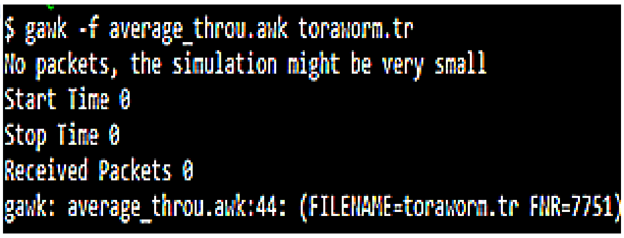
Packet Delivery Ratio for TORA was executed with gawk –f pdr.awk toraworm.tr command resulted in an output in fig 5

Average Throughput for TORA was executed with gawk –f average_throughput.awk toraworm.tr command, resulted in an out in figure 6



```
$ gawk -f pdr.awk toraworm2.tr
the sent packets are 1251
the received packets are 0
the forwarded packets are 0
Packet Delivery Ratio is 0.000000
```

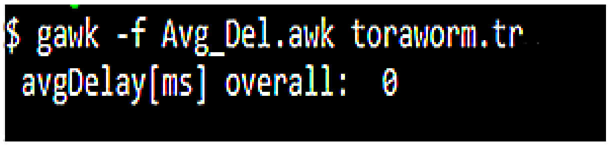
Fig: 5 Packet delivery ratio for TORA



```
$ gawk -f average_throu.awk toraworm.tr
No packets, the simulation might be very small
Start Time 0
Stop Time 0
Received Packets 0
gawk: average_throu.awk:44: (FILENAME=toraworm.tr FNR=7751)
```

Fig: 6 Average throughput for TORA

Average delay for TORA was executed with gawk –f Avg_Delay.awk toraworm.tr command, resulted in an output in fig 7.

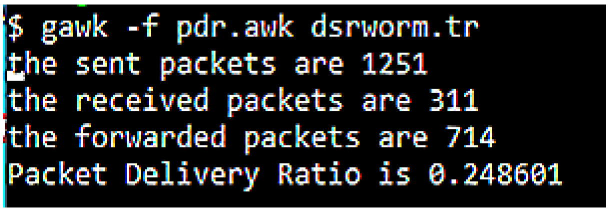


```
$ gawk -f Avg_Del.awk toraworm.tr
 avgDelay[ms] overall:  0
```

Fig: 8 Average delay for TORA

3.4.3 Simulation Experiment and Output for DSR

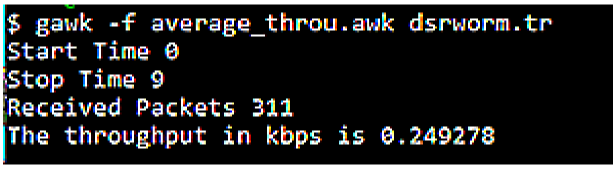
With the same settings, Packet Delivery Ratio for DSR was executed with gawk –f pdr.awk dsrworm.tr command which resulted in an output shown in Fig. 9.



```
$ gawk -f pdr.awk dsrworm.tr
the sent packets are 1251
the received packets are 311
the forwarded packets are 714
Packet Delivery Ratio is 0.248601
```

Fig 9: Packet delivery ratio for DSR

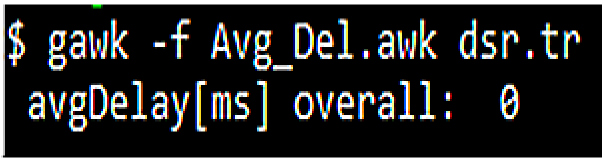
Average Throughput for DSR was executed with gawk –f average_throughput.awk dsrworm.tr command which resulted in an output shown in Fig. 10.



```
$ gawk -f average_throu.awk dsrworm.tr
Start Time 0
Stop Time 9
Received Packets 311
The throughput in kbps is 0.249278
```

Fig: 10. Average Throughput for DSR

Average delay for DSR was executed with gawk –f Avg_Delay.awk dsrworm.tr command resulting in an output shown in Fig. 11.



```
$ gawk -f Avg_Del.awk dsr.tr
 avgDelay[ms] overall:  0
```

Fig: 11 Average delay for DSR

4. RESULTS AND DISCUSSIONS

Based on the simulation results, the average throughput for the DSDV and TORA protocols was 0, while for the DSR protocol it was measured at 0.2492. The packet delivery ratio for both the DSDV and TORA protocols was 0%, indicating that no packets reached the destination successfully, whereas for the DSR protocol, the packet delivery ratio was 24.86%. Furthermore, the average end-to-end delay for both the DSDV and TORA protocols was 0, indicating no delay in packet transmission, whereas for the DSR protocol, the average end-to-end delay was measured at 1.523 milliseconds, as shown in Table 3.

Table 3 Simulation results

Metrics	Routing Protocols		
	DSDV	TORA	DSR
Average throughput	0	0	0.2492
Packet delivery ratio	0%	0%	24.86%
Average end to end delay	0	0	1.523ms

4.1 Average Throughput Analysis

The average throughput for DSDV and TORA routing protocols was observed to be zero packets, which can be attributed to potential wormhole attacks that result in nil or very little data delivery. The DSR protocol, on the other hand, displayed a noteworthy average throughput of 0.2492, indicating a significantly higher amount of successful data transmission and a stronger resistance to wormhole attacks, as shown in Fig 12.

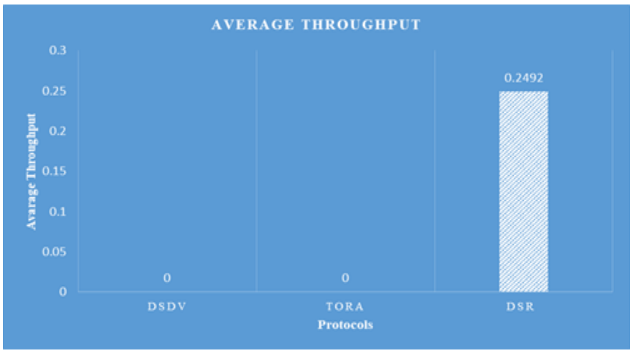


Fig: 12 Average throughput graph

4.2 Packet delivery ratio

The DSDV and TORA routing protocols had a 0 packet delivery ratio, suggesting no successful or low transfer rates. However, the DSR protocol had a 0.2486 ratio, indicating a higher success and survival rate in delivering packets to intended destinations, even with potential wormhole attack threats, as shown in figure 13.

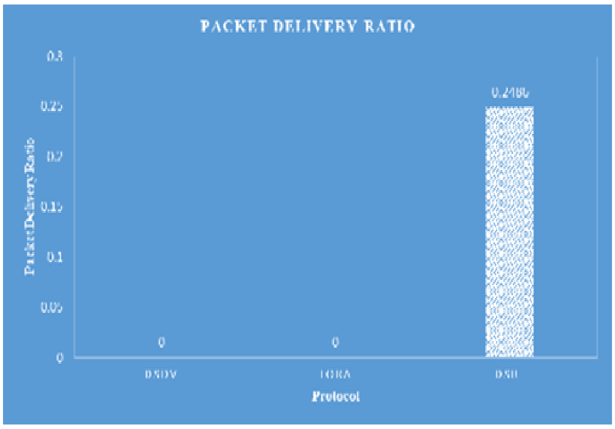


Fig: 13 Packet delivery ratio

4.3 Average end-to-end delay

The DSDV and TORA routing protocols had no measurable or negligible end-to-end delay, possibly due to wormhole attacks. The DSR protocol had an average end-to-end delay of 1.523 ms, suggesting a slight delay in packet delivery, possibly influenced by wormhole attacks, as shown in Fig. 14.

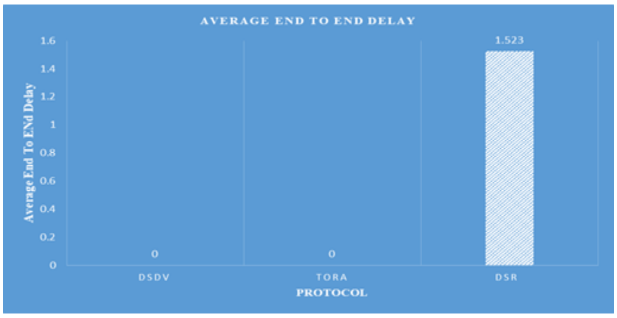


Fig: 14 Average End-to-End Delay

5. CONCLUSION

The NS-2 simulator's simulation results were analysed to compare and evaluate the performance of DSR, DSDV, and TORA protocols. The results showed that wormhole attacks severely affected the DSDV and TORA routing protocols, causing a lack of data transmission and a poor packet delivery ratio. However, the DSR protocol showed better performance with a higher average throughput, indicating successful data transmission and improved resistance against wormhole attacks. The DSR protocol shows a slight delay, possibly influenced by wormhole attacks, emphasizing robust routing for efficient data transfer in mobile ad hoc networks.

The future research trajectory for this study will focus on exploring alternative performance metrics, assessing a spectrum of routing protocols, scrutinising the implications of diverse attack scenarios, refining and augmenting security mechanisms to thwart attacks on Mobile Ad-Hoc Networks (MANETs), undertaking real-world experiments, and implementing protocols aimed at optimising the efficiency of MANET routing mechanisms.

6. ACKNOWLEDGMENTS

We express our gratitude to the reviewers for their thorough examination of the paper as well as their valuable comments and suggestions that significantly enhanced the quality of the manuscript. Also, our gratitude goes to Kwame Nkrumah University of Science and Technology (KNUST) Kumasi, Valley View University, Accra, Ghana, and the University of Cincinnati Ohio, USA

7. REFERENCES

[1] E. Setijadi, I. K. E. Purnama, and M. H. Pumomo, "Performance comparative of AODV, AOMDV and DSDV routing protocols in MANET using NS2," in *2018 international seminar on application for technology of information and communication*, 2018: IEEE, pp. 286-289.

[2] E. Setijadi, I. K. E. Purnama, and M. H. Pumomo, "Performance comparative of AODV, AOMDV and DSDV routing protocols in MANET using NS2," in 2018 international seminar on application for technology of information and communication, 2018: IEEE, pp. 286-289.

[3] N. Panda, B. Patra, and S. Hota, "Manet Routing Attacks and Their Countermeasures: A Survey," J. Crit. Rev, vol. 7, pp. 2777-2792, 2020.

[4] F. H. Shajin and P. Rajesh, "Trusted secure geographic routing protocol: outsider attack detection in mobile ad hoc networks by adopting trusted secure geographic routing protocol," International Journal of Pervasive Computing and Communications, vol. 18, no. 5, pp. 603-621, 2022.

[5] M. Tahboush and M. Agoyi, "A hybrid wormhole attack detection in mobile ad-hoc network (MANET)," IEEE Access, vol. 9, pp. 11872-11883, 2021.

[6] B. B. Gupta and A. Dahiya, Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures. CRC press, 2021.

[7] E. Ochola, L. Mejaele, M. Eloff, and J. Van Der Poll, "Manet reactive routing protocols node mobility variation effect in analysing the impact of black hole attack," SAIEE Africa Research Journal, vol. 108, no. 2, pp. 80-92, 2017.

[8] M. T. Sultan, H. El Sayed, and M. A. Khan, "Performance Analysis of the Impact of DDoS Attack on Routing Protocols in Infrastructure-less Mobile Networks," in 2022 5th International Conference on Communications, Signal Processing, and their Applications (ICCSPA), 2022: IEEE, pp. 1-6.

[9] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," Ad Hoc Networks, vol. 133, p. 102894, 2022.

[10] Y. Zhuang, Y. Wang, Y. Yan, X. Xu, and Y. Shi, "Reflectrack: Enabling 3d acoustic position tracking using commodity dual-microphone smartphones," in The 34th Annual ACM Symposium on User Interface Software and Technology, 2021, pp. 1050-1062.

[11] A. Mchergui, T. Moulahi, and S. Zeadally, "Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (VANETs)," Vehicular Communications, vol. 34, p. 100403, 2022.

[12] A. Norén-Nilsson, "Youth mobilization, power reproduction and Cambodia’s authoritarian turn," Contemporary Southeast Asia, vol. 43, no. 2, pp. 265-292, 2021.

[13] A. Srivastava and J. Prakash, "Future FANET with application and enabling techniques: Anatomization and sustainability issues," Computer science review, vol. 39, p. 100359, 2021.

[14] A. C. J. Malar, M. Kowsigan, N. Krishnamoorthy, S. Karthick, E. Prabhu, and K. Venkatachalam, "Multi constraints applied energy efficient routing technique based on ant colony optimization used for disaster resilient location detection in mobile ad-hoc network," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 4007-4017, 2021.

[15] M. Rajhi, H. Madkhali, and I. Daghriri, "Comparison and analysis performance in topology-based routing protocols in vehicular ad-hoc network (VANET)," in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021: IEEE, pp. 1139-1146.

[16] S. Sarhan and S. Sarhan, "Elephant herding optimization Ad Hoc on-demand multipath distance vector routing protocol for MANET," IEEE Access, vol. 9, pp. 39489-39499, 2021.

[17] G. Kaur and P. Thakur, "Routing protocols in manet: An overview," in 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 2019, vol. 1: IEEE, pp. 935-941.

[18] S. Basu et al., "A Comparative Study on Propagation Models for Routing Protocols in FANETs," in 2021 IEEE International India Geoscience and Remote Sensing Symposium (InGARSS), 2021: IEEE, pp. 528-531.

[19] P. K. Shrivastava and L. Vishwamitra, "Comparative analysis of proactive and reactive routing protocols in VANET environment," Measurement: Sensors, vol. 16, p. 100051, 2021.

[20] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "Computer network simulation with ns-3: A systematic literature review," Electronics, vol. 9, no. 2, p. 272, 2020.

[21] T. K. Saini and S. C. Sharma, "Prominent unicast routing protocols for Mobile Ad hoc Networks: Criterion, classification, and keyattributes," Ad Hoc Networks, vol. 89, pp. 58-77, 2019.