Identifying the Impacts of Active and Passive Attacks on Network Layer in a Mobile Ad-hoc Network: A Simulation Perspective

Uthumansa Ahamed[1]
Department of Physical Sciences
Faculty of Applied Sciences
Rajarata University of Sri Lanka
Mihintale, Sri Lanka

Shantha Fernando[2]
Department of Computer Science
& Engineering, Faculty of Engineering
University of Moratuwa
Moratuwa, Sri Lanka

***Abstract*—In this research, we attempted to investigate about the features and behaviors of network layer based active and passive attacks in Ad-hoc On-Demand Vector (AODV) routing protocol in Mobile Ad-hoc Networks (MANET). Through the literature survey, we try to understand the features of each attacks and examine the behaviors of these attacks through simulations via Network Simulator 2 (NS2). Blackhole, Grayhole and Wormhole attacks are used in this simulation study. Each attacks are introduced independently into the network to find the impacts on network performances that are evaluated through Packet Delivery Ratio (PDR), Average End-to-End Delay (AEED), Throughput, Average Data Dropping Rate (ADDR) and Simulation Processing Time at Intermediate Nodes (SPTIN). To obtain more accurate results, simulation parameters are maintained same in each simulation. A controller network is simulated to compare with each attack simulation. Simulations are repeated by changing the number of connected intermediate nodes (hops) in the network. We observed at collected data analysis, the lowest SPTIN in the network that contained a Blackhole or Grayhole attack out of these three attacks. The network which is affected by a Blackhole attack shows higher amount of ADDR than controller network. Furthermore data forwarding rate is higher in the network which is affected by a Wormhole attack. Finally, according to the simulation studies, we are able to understand that Blackhole and Grayhole attacks cause more damage to the network performances than Wormhole attacks.**

***Keywords*—Active attack; network layer; passive attack; performance matrices; simulation study**

I. Introduction

4G technology allows devices to communicate each other through wireless medium even at the absence of predefined infrastructure networks. These wireless devices are capable of making connections between themselves when they are capable to listen to one-another. This type of network is called an Ad Hoc Network [1]. MANET is a type of wireless ad hoc network. In MANET, each device is defined as a node and fundamental feature of a MANET is node mobility. Mainly three different types of nodes are available in MANET. Those are source node, destination node and routing (intermediate) node. In pure MANET paradigm, there is no fixed infrastructure. Usually nodes can join and leave from the network without any constrain. Therefore, network topology changes eventually. Another important feature of a node in MANET is limited radio range which leads to depend on the help of neighbouring nodes (multi-hop) to communicate with destination node when source and destination nodes are not in their radio range. Furthermore, nodes use Open Systems Interconnection (OSI) model standards to communicate among them. Because of multi-hop nature nodes often act not only as hosts but also as routers. In a multi-hop network one or more intermediate nodes are possible to connect in a route between source and destination [1]–[3]. This opportunistic nature of MANET made attention to use on military and rescue agencies particularly under disorganized or hostile environments where services of infrastructure networks are unavailable because of disaster situations [2]. Relatively low cost on network deployment made MANET a more common and smart alternative even for commercial uses such as virtual classrooms [3].

Open network boundary, infrastructure-less nature and dynamic network topology are some fundamental characters of a MANET. These characters expose MANET into different types of security attacks on each OSI layers and routing protocols are operated on Network layer of OSI model. Routing protocols in the MANET can be categorized into Two: Proactive and Reactive. Proactive routing protocols need to maintain routing information even if there are no demand for a communication [4]–[6]. These types of protocols are only suitable for stationary and fewer number of nodes [7]. Reactive routing protocols start to find a route to destination only for a demand. There are no any routing details at the beginning [8]. Hybrid routing protocols are combination of proactive and reactive routing protocols. Still it has the limitation of Proactive routing protocols [7], [9].

Furthermore, most of the routing protocols (e.g.: AODV) are working based on the trustworthiness of each node. “All nodes are reliable” is the main assumption of pure routing protocols [8]. Therefore, attacking node can be a part of a MANET easily. Most routing protocols perform well, but fail to address the network security. Therefore security attacks are needed to be addressed to protect the network performances during the data communication through the network. This research is aimed to identify the impacts of active and passive attacks on network layer in a MANET. Outcomes of this research will be help to re-design routing protocol with an adaptive model to handle network layer attacks in MANET.

The rest of this paper is organized as follows. State of

the art of the network layer attacks is presented on Section 2. Different network layer attacks on AODV protocol are described in Section 3. Our research methodology explains in Section 4. In Section 5, we present our simulation results and discussion. Summary of analysis and discussion is included in Section 6. Finally, Section 7 explains about the conclusion and future works.

II. State-of-the-Art

Authors in [10] proposed classifications of different security attacks on a MANET. It is helpful for better understanding of each attack. The affects of Wormhole attack on few routing protocols were summarized by authors in [11]. Furthermore, detailed comparative analysis on detection and prevention techniques of Wormhole attack is presented in the same research, though this study does not carryout any simulation study. Authors in [12] presented a study on Wormhole attack prevention techniques and a simulation study on Wormhole attack on AODV and DSR routing protocols and few simulation results are unclear about the Wormhole attack which is applied on AODV or DSR. Authors in [13] discussed about state of the art on prevention mechanisms of Blackhole attack. In [14] surveyed some of the existing solutions for Blackhole, Grayhole and Wormhole attacks. Authors in [15] simulated four different types of routing attacks (Active attacks) but their simulation results contradict with their Blackhole attack definition. According to the definition in their research paper, Blackhole attack drops all the packet what it receives except Routing Request (RREQ) packets even though their simulation results show considerable amount of data transaction in the presence of Blackhole attack. Authors in [16] conducted a study on few network layer attacks and routing protocols. Finally, they suggested some solutions for routing protocols to overcome network layer attacks through the literature survey. In [17] they presented a survey of significant network layer attacks and review of intrusion detection mechanisms that have been proposed in the literature. Authors in [18] reviewed mitigation of various routing attacks and prevention on these attacks. Authors in [19] presented a study on Blackhole attack through inducting malicious node activity in AODV under different scenarios. In [20] they investigated some security issues in MANET as well as countermeasures against such attacks in existing MANET protocols.

Most of these studies rely only on the theoretical findings. Therefore, it is difficult to identify the impact of active and passive attacks on MANET. Furthermore, it is difficult to understand the impact of each attack separately on the network performances. Therefore it is important to conduct a simulation study on attacks in order to identify the impacts of active and passive attack to propose a better countermeasure on network layer attacks.

III. Network Layer Attacks on AODV

The primary function of the network layer is routing [21]. In MANET most of the attacks are delivered after accessing the routing information [22]. The followings are some examples for network layer attacks [20], [23].

1) Blackhole Attack
2) Grayhole Attack
3) Wormhole Attack
4) Routing Table Overflow
5) Byzantine Attack
6) Link Spoofing Attack

In Blackhole attack malicious node which is the originator of the attack sends reply having destination sequence number in maximum possible value and hop count in minimum value during route discovery. Then source establishes a path including malicious node as router in it. In this path, destination may be found or may not. Then all the traffics will be redirected by the malicious node. Moreover, the route established by the malicious node starts to drop rather than deliver or retransmit when it receives data. It is possible to appear one or more malicious nodes in a route [20], [24].

Grayhole attack can be described as an extension of Blackhole attack. Attacking node behaves as a genuine node as well as a malicious node. During a communication between source node and destination node, attacking node acts as a genuine node by delivering or retransmitting what is received. To some period it drops all packets that it receives. In some other cases, attacker node drops data packets from a specific node and forward or retransmit data packets from other nodes.

Minimum two or more nodes are involved in a Wormhole attack. A private link (called as Wormhole tunnel) is established in-between these malicious nodes. These nodes may get themselves involved in more routes. Imitate with shortest path to source node during route discovery. When they become a router in a route, start to exploit data packet that they received. Wormhole nodes can drop, modify or send data packets to third party for malicious purpose. It is difficult to detect because of its cooperative nature [25], [26].

Furthermore, Blackhole and Grayhole attacks are categorized as Active attacks which disrupt the network performances and collapse the network. Wormhole attack is categorized as Passive attack which do not harm the network performances but collects or steals data which are needed to form an Active attack from the network. Rather than most of the network layer attacks listed above, Blackhole, Grayhole and Wormhole attacks (Hole attacks) behave relatively in similar manner. Following are some similarities between these Hole attacks.

- All of these attacks are network layer oriented [16], [20].
- Deliver false details during the routing discovery [16], [20], [24].
- Each attack intentionally drops packet during the session [16], [20], [23].
- During the session each attack shows misbehaving activity [14], [16], [20].
- During the attack, single node involves to alter data packets [14], [20].
- Routing protocol mislead by each attack [14], [16], [20], [24].
- Each attack advertises fake route during routing discovery [16], [20].

TABLE I. DIFFERENCES BETWEEN ATTACKS

Feature	Blackhole Attack	Grayhole Attack	Wormhole Attack
No of nodes need to form an attack	One node [20], [24]	One node [14]–[17], [25]	Two nodes [12], [20] [23], [25]
Attack type	Active [13], [23], [24]	Active [14]–[17], [25]	Passive [25]
Ability to communicate with destination node	Can not [13], [24]	Can [14], [16] [25], [27]	Can [12], [20], [25]
Attacker position	Part of the network [13], [20]	Part of the network [14]–[17], [25]	Both in the same network or different networks [25]
Data in RREP packets	False data [13], [20] [24], [26]	True data [14], [25], [26]	False or true data [28]
Data packet forwarding and transmission	Drops all data packets that that it receives [13], [23], [24]	Drops only selected data packets or drop only data packets from precise node [14], [16], [25]	Eventually drop data packets or forward or retransmit as normal node [28]
Network performance	Entire network will collapse [13], [20], [24]	will be reduced or network collapse after some period [14]–[16] [24], [25]	will be reduced but network will not collapse [28]

Table I shows differences and unique features between these attacks. Because of these unique features of each attack, they differ from one another.

IV. METHODOLOGY

During the research, NS2 is used as the test bed to simulate different scenarios. Table II shows simulation parameters maintained in NS2 during the simulations. For more accuracy, readings are recorded by changing the number of connected intermediate nodes (10, 15, 20, 25 and 30) at each simulation and different attacks are introduced into the network to check the impacts on the Performance Matrixes (PM): PDR, AEED and Throughput. In addition, performance on ADDR and SPTIN also have studied to understand more about each attacks. The attacks are injected by modifying the AODV routing protocol.

Each attack is introduced to the network individually to check the impacts separately. Furthermore, a network without any attack is simulated as the controller. Impact on each attacks are analyzed with respect to the controller. Recorded data are analyzed in Tracegraph 2.02 and visualized in Microsoft Office Excel 2007. During the simulations following assumptions are considered.

- All nodes were considered to be identical in software and hardware configurations.
- All the nodes except malicious nodes show no any malicious behavior during the data communication.

TABLE II. NS2 SIMULATION PARAMETERS

Simulation parameter	Value
Simulator	NS2 (v.2.34)
Number of nodes	10, 15, 20, 25, 30
Transmitter range	250 m
Bandwidth	2.0 x 10^6 bps
Frequency	9.14 x 10^8 Hz
Antenna/OmniAntenna X, Y, Z	0, 0, 1.5 m
Traffic type	Constant bit rate (CBR)
Radio-propagation model	TwoRayGround
Network interface type	Phy/WirelessPhy
Routing protocol	AODV
Max packets in Interface Queue	50
Time of simulation	5 s
Mobility model	None

V. SIMULATION RESULTS AND DISCUSSION

In order to investigate on the impacts of each Hole attacks, network performances evaluate with PDR, EED and Throughput. Furthermore, test result analysis with another two different parameters: ADDR; SPTIN.

A. PDR

PDR is a ratio between successfully received packets and total number of packets sent by the sender. PDR then is multiplied by 100 to obtain as a percentage [29]. A graph is plotted by using simulation results for PDR vs. number of connected nodes in the network. It is illustrated in Fig. 1.

$$PDR = \frac{Successfully\ received\ packets}{Total\ number\ of\ sent\ packets} \times 100 \quad (1)$$

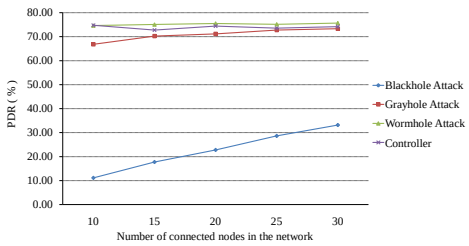

Fig. 1. Graph of PDR vs. Number of Connected Nodes in the Network.

According to the simulated results, controller network shows 73.75% of average PDR rate. The network with Wormhole attack shows a higher average PDR value, which is 75.19%. The reason for this is the communication between the attacker nodes via a Wormhole tunnel. This shows higher data flow through Wormhole tunnel. The network which is affected by Grayhole attack shows 70.85% of PDR value. The network which is affected by Blackhole attack shows lower PDR. The average PDR value is 22.69%. This is because attacker node drops the entire packets that it receives except AODV routing packets. But when the number of connected nodes in the

network increases, PDR value also increases. This is because when the number of connected nodes in the network increases, routing protocol is sending to find the route by sending more RREQ packets.

B. AEED

$$AEED = \frac{Total\ no\ of\ packets\ reached\ by\ destination\ node}{Total\ time\ taken\ to\ receive\ all\ packets\ by\ destination\ node} \quad (2)$$

End-to-End Delay is an amount of the time which is taken by a packet to reach destination node from the source node. Unit is seconds [20], [29]. Fig. 2 shows the graph which is plotted for AEED vs. number of connected nodes in the network. Controller network shows higher AEED value and when the number of nodes increases the value gradually increases. This is because when the number of nodes increases in the network, data packets need to pass through more intermediate nodes to reach the destination node. Average value of a given number of nodes in the network is used to plot the graph in Fig. 2. Furthermore, mean value of each AEED is 0.096634435696 seconds.

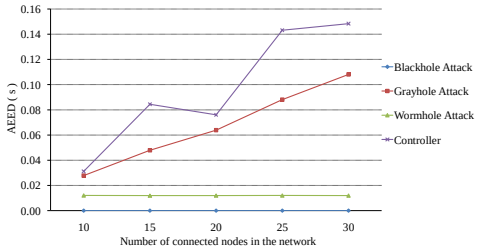

Fig. 2. Graph of AEED vs. Number of Connected Nodes in the Network.

The lowest AEED value is shown in the presence of Blackhole attack because there are no any data packets available to reach at the destination node. All the data packets are dropped by the attacker node in the network. Therefore, AEED value is not available. This is assumed as 0 for each number of nodes in the network for the graphing purpose. AEED value of the network which is affected by Grayhole attacks is lower than the value of the controller network. When the number of nodes increases in the network, AEED value increases gradually. However, it is still lower than the AEED value of controller network. Data packets communication speed through this network is 1.43 times faster than the speed in controller network. The mean value of all AEED of the network which is affected by Grayhole attack is 0.067165942022 seconds.

In the presence of a Wormhole attack data forwarding speed is abnormally faster than the controller. It is because of the faster connection in between two Wormhole nodes. Therefore, this network shows the lowest AEED value. According to the simulation results, the mean value of all AEED value is 0.012056294606 seconds. Therefore, data transferring speed is 8 times faster than the controller network. However, during a Wormhole attack, increment of the number of connected nodes in the network is not affected by AEED value. Therefore, the value is quiet similar in each scenario.

C. Throughput

$$Throughput = \frac{Total\ number\ of\ packets\ received\ by\ destination\ node}{Total\ time\ taken\ to\ receive\ packets} \quad (3)$$

This is an important measure to check the performance of the network. This value is a ratio which is calculated as Eq 3 by total number of packets received by destination node over total time taken to receive all packets. Units are bytes per second (bps).

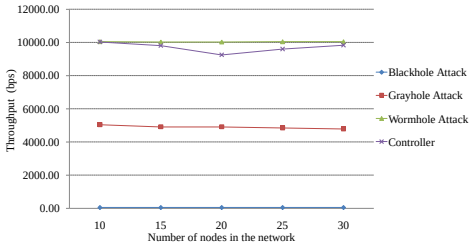

Fig. 3. Graph of Throughput vs. Number of Connected Nodes in the Network.

Fig. 3 shows a graph that is plotted between throughput vs. number of connected nodes in the network. The average throughput is 9706 bps. This is the 80.95 % of total data sent by source node. The network which is affected by Wormhole attack shows higher amount of throughput than controller network. The average throughput value is 10040 bps which is 83.92% of total data sent by source node. The lowest throughput value is recorded as 45 bps when a Blackhole attack is affected on a network. These amounts of routing data allow through Blackhole node. When Grayhole attack is affected on a network then the throughput amount will be lower than controller network and higher than Blackhole attack affected network. The average value is 4897 bps. The 41.03% of sent data from source node is received by destination node. Each network which is affected by any attack including controller network shows throughput decreasing while increasing the number of connected nodes in the network.

D. ADDR

$$ADDR = \frac{Total\ average\ data\ dropping\ rate\ of\ all\ nodes}{Simulation\ time} \quad (4)$$

Fig. 4 is a graph that shows average data dropping rate of a network. Graph plotted between ADDR vs. number of connected nodes in the network. Controller network shows 1091.34 bps as average ADDR. The ADDR value of the controller network increases by increasing the number of connected nodes in the network. The lowest average of ADDR value is recorded when Wormhole attack is affected on a network. It is 116.52 bps. This is 1/10 lower than controller networks' value. Furthermore, when number of connected nodes in the network increases, the ADDR decreases, because of the affect of a Wormhole attack. The higher average of

ADDR values is observed when a network is affected by a Blackhole attack. It is 8674.83 bps. This is 8 times higher than ADDN value of controller network. These affected networks do not show remarkable increase or decrease in ADDR during the change of number of connected nodes in the network. When a Grayhole attack is affected on a network, it shows 4350.73 bps. This is 4 times higher than ADDN value of controller network. Furthermore, when number of connected node increases the ADDN value also increases. The highest ADDR values are shown in the presence of Blackhole attack and the mean value of ADDR values is 0.106 bps. This means when a Blackhole attack is presented in a network, it drops data 106 times than a network without a Blackhole attack. The networks which are affected by a Grayhole attack show 0.008 bps of mean value for all ADDR value on the network.

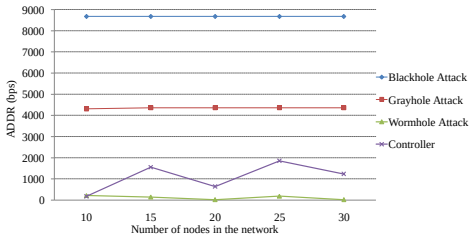

Fig. 4. Graph of ADDR vs. Number of Connected Nodes in the Network.

E. SPTIN

$$SPTIN = \frac{Total\ processing\ times\ of\ connected\ nodes\ in\ the\ network}{No\ of\ connected\ nodes\ in\ the\ network} \quad (5)$$

Fig. 5 is a graph which is plotted between SPTIN and number of connected nodes in the network. According to the graph, the SPTIN value of the controller network is 0.0137 seconds. The network which is affected by Balckhole attack shows higher amount of SPTIN. The average SPTIN value is 0.0570 seconds. It is nearly 4 times higher than SPTIN value of the controller network. Lower average SPTIN value is observed at the network which is affected by Wormhole attack. It is 0.0006 seconds. This is 20 times lower than average SPTIN value of the controller network. Average SPTIN value is 0.0020 seconds when a network is affected by Grayhole attack. This value is 7 times lower than average SPTIN value of controller network. All networks show relatively similar SPTIN value at the lowest number of connected nodes in the network except the network which is affected by a Blackhole attack. Furthermore, the linear trendline for all SPTIN value of the controller networks, Blackhole and Grayhole attack affected networks show gradual increase of SPTIN value with increase of the number of connected nodes in the network. However, when Wormhole attack is affected on a network, the SPTIN values of the networks are relatively same while the number of connected nodes in the network is increasing.

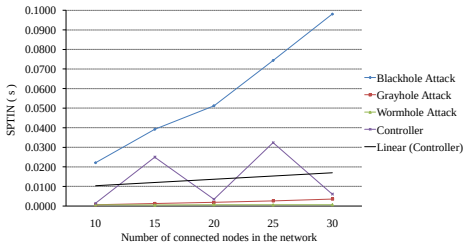

Fig. 5. Graph of SPTIN vs. Number of Connected Nodes in the Network.

VI. Summary of Analysis and Discussion

Table III shows summary of analyzed results. All values are converted into a percentage value with respect to the value of controller network. In Active attacks, Blackhole attacks causes severe damage to a network performances than Grayhole attack. Although performances of a network which is affected by a Grayhole attack varies in between the performances of the network which is affected by Blackhole attack and performances of the controller network. Furthermore, there are significant amount of enhancement of the network performances on the network by the affect of a Wormhole attack. Among the reactive routing protocols, AODV routing protocol performs well [5], [30]–[32]. Therefore, AODV routing protocol is used for network simulations in this research.

TABLE III. Summary of Analyzed Data

Network parameter	Controller (%)	Blackhole (%)	Grayhole (%)	Wormhole (%)
PDR	73.75	22.69	70.85	75.19
AEED	100.00	∞	69.51	12.48
Throughput	80.95	0.38	41.03	83.92
ADDR	100.00	10.68	398.66	794.88
SPTIN	100.00	416.75	14.74	4.68

VII. Conclusion and Future Works

According to the simulation results, we can conclude that active attacks are more destructive than passive attacks. In an Active attack, malicious node drops data packets. Though in a passive attack, malicious nodes provide better performances than as usual to become a part of the network. The reason for higher performance is Wormhole tunnel.

AODV routing protocol is more suitable for MANET. Pure AODV protocol is only considering about data communication but not data security. In AODV routing protocol, most of the malicious nodes become a part in the network at initial route discovery process. Therefore, node selection process for a network must be more qualitative and precise by concerning on data security. Furthermore, in MANET a routing protocol can be able to identify affects of Hole attacks therefore it is possible to apply suitable mechanisms to prevent these attacks through the routing protocol. Therefore, routing protocol should be equipped with an adaptive model which includes different suitable security mechanisms to prevent and handle the Hole attacks. In our future work, we intend to modify AODV protocol with an adaptive model to prevent these Hole attacks.

REFERENCES

[1] H. Xu, Y. Zhao, L. Zhang, J. Wang, "A Bio-Inspired Gateway Selection Scheme for Hybrid Mobile Ad Hoc Networks," *IEEE Access,* vol. 7, pp. 61997-62010, 2019, doi: 10.1109/ACCESS.2019.2916189

[2] L. Khoukhi, H. Badis, L. Boulahia, M. Esseghir, "Admission control in wireless ad hoc networks: a survey," *EURASIP Journal on Wireless Communications and Networking,* vol. 109(2013), pp. 1-13, 2013, doi: 10.1186/1687-1499-2013-109

[3] H. Deng, W. Li, D. Agarwal, "Routing security in wireless ad-hoc networks," *IEEE Communication Magazine,* vol. 40 (10), pp. 70-75, 2002, doi: 10.1109/MCOM.2002.1039859

[4] N. Brahmi, M. Boussedjra, J.Mouzna, "Routing in vehicular ad hoc networks: towards road-connectivity based routing," in *Mobile Ad-hoc Networks: Applications,* X. Wang, Ed. Janeza Trdine, Rijeka, Croatia: InTech, 2011. pp. 89-106.

[5] T. Nakashima, "Theory and applications of ad hoc networks," in *Mobile Ad-Hoc Networks: Protocol Design*, X. Wang, Ed. Janeza Trdine, Rijeka, Croatia: InTech, 2011. pp. 615-638.

[6] A. Ade, P. Tijare, "Performance comparison of AODV, DSDV, OLSR and DSR routing protocols in mobile ad hoc networks," *International Journal of Information Technology and Knowledge Management 2010,* vol. 2 (2), pp. 545-548, 2010, doi:10.1109/PDGC.2016.7913218

[7] M. Kang, D. Kum, J. Bae, Y. Cho, A. Le, "Mobility aware routing protocol for mobile ad hoc network" in *2012 International Conference on Information Networking,* Dresden, Germany: IEEE, 2012. pp. 410-414, doi: 10.1109/ICCW.2009.5208062

[8] C. Perking, E. Royer, "Ad-hoc on-demand distance vector routing," in *2nd IEEE Workshop on Mobile Computing Systems and Applications,* New Orleans, LA, USA: IEEE, 1999. pp. 90-100.

[9] L. He, J. Huang, F. Yang, "A noval hybrid wireless routing protocol for WMNs," *2010 International Conference on Electronics and Information Engineering,* Kyoto: IEEE, 2010. pp. 281-285, doi: 10.1109/ICEIE.2010.5559874

[10] R. Meddeb, B. Triki, F. Jemili, O. Korbaa, "A survey of attacks in mobile ad hoc networks," *2017 International Conference on Engineering & MIS (ICEMIS),* Monastir: IEEE, 2017, pp. 1-7, doi: 10.1109/ICEMIS.2017.8273007

[11] S. Banerjee, K. Majumder, "A Comparative Study on Wormhole Attack Prevention Schemes in Mobile Ad-Hoc Network," in *Recent Trends in Computer Networks and Distributed Systems Security. SNDS 2012. Communications in Computer and Information Science,* M. Thampi, Y. Zomaya, T, Strufe, A. Calero, T. Thomas, Eds. Berlin, Heidelberg: Springer, 2012, pp. 372–384, doi: 10.1007/978-3-642-34135-9_37

[12] R. Maulik, N. Chaki, "A comprehensive review on wormhole attacks in MANET," in *2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM),* Krackow: IEEE, 2010, pp. 233-238, doi: 10.1109/CISIM.2010.5643657

[13] F. Tseng, L. Chou, H. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," in *Human-centric Computing and Information Sciences 1,* Thaiwan: Springer, 2011, vol. 4 (2011), doi: 10.1186/2192-1962-1-4

[14] H. Jhaveri, J. Patel, C. Jinwala, "DoS Attacks in Mobile Ad Hoc Networks: A Survey," in *2012 Second International Conference on Advanced Computing & Communication Technologies,* Rohtak, Haryana: IEEE, 2012, pp. 535-541, doi: 10.1109/ACCT.2012.48

[15] A. Abdelshafy, B. King, "Analysis of security attacks on AODV routing," in *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013),* London: IEEE, 2013, pp. 290-295, doi: 10.1109/ICITST.2013.6750209

[16] A. Saeed, A. Raza, H. Abbas, "A Survey on Network Layer Attacks and AODV Defense in Mobile Ad Hoc Networks," in *2014 IEEE Eighth International Conference on Software Security and Reliability-Companion,* San Francisco, CA: IEEE, 2014, pp. 185-191, doi: 10.1109/SERE-C.2014.37

[17] A. Nadeem, P. Howarth,"A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," in *IEEE Communications Surveys & Tutorials,* Guildford, UK: IEEE, 2013, vol. 15, no. 4, pp. 2027-2045, doi: 10.1109/SURV.2013.030713.00201

[18] M. Karthigha, L. Latha, K. Sripriyan, "A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks," in *2020 International Conference on Inventive Computation Technologies (ICICT),* Coimbatore, India: IEEE, 2020, pp. 396-402, doi: 10.1109/ICICT48043.2020.9112588

[19] A. Aggarwal, N. Chaubey, A. Jani, "A simulation study of malicious activities under various scenarios in Mobile Ad hoc Networks (MANETs)," in *2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)*, Kottayam, India: IEEE, 2013, pp. 827-834, doi: 10.1109/iMac4s.2013.6526521

[20] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kaito, A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," in *IEEE Wireless Communications,*: IEEE, 2007, vol. 14 (5), pp. 85-91, doi: 10.1109/MWC.2007.4396947

[21] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, D. Gaiti, "Flooding attacks detection in MANETs," in *2015 International Conference on Cyber Security of Smart cities (SSIC),* Shanghai, China: IEEE, 2015. pp. 1-6, doi: 10.1109/SSIC.2015.7245675

[22] S. Djahel, F. Abdesselam, A. Khokhar, "A cross layer framework to mitigate a joint MAC and routing attack in multihop wireless networks," in *2009 IEEE 34th Conference on Local Computer Networks,* Zurich, Switzerland: IEEE, 2009. pp. 730-737, doi: 10.1109/LCN.2009.5355066

[23] J, Karlsson, L. Dooley, G. Pulkkis, "Secure routing for MANET connected internet of things systems," in *IEEE International Conference on Future Internet of Things and Cloud,* Barcelona, Spain; IEEE, 2018. pp. 114-119.

[24] G. Li, Z. Yan, Y. Fu, "A study and simulation research of blackhole attack on mobile adhoc network" in *2018 IEEE Conference on Communications and Network Security (CNS),* Beijing, China; IEEE, 2018. pp. 1-6.

[25] R. Mehta, M. Parmar, "Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole &Grayhole Attacks," in *2018 3rd International Conference for Convergence in Technology (I2CT)* Pune, India: IEEE, 2018, pp. 1-6.

[26] P. Roshani, A. Patel, "Techniquesto mitigate grayhole attack in MANET: a survey," in *2017 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS),* Coimbatore, India: IEEE, 2017, pp. 1-4.

[27] K. Ullah, P. Das, "Trust-based routing for mitigating grayhole attack in MANET," in *Proceedings of the International Conference on Computing and Communication Systems, Lecture Notes in Networks and Systems* J. Mandal, G. Saha, D. Kandar, A. Maji, Eds. Singapore: Springer Singapore, 2018. pp. 713-721, doi: 10.1007/978-981-10-6890-4_68

[28] M. Patel, A. Aggarwal, N. Chaubey, "Analysis of Wormhole Attacks in Wireless Sensor Networks," in *Recent Findings in Intelligent Computing Techniques. Advances in Intelligent Systems and Computing,* P. Sa, S. Bakshi, I, Hatzilygeroudis, M. Sahoo, Eds. Springer-Singapore: Springer, 2018, vol. 708, doi: 10.1007/978-981-10-8636-6_4

[29] M. Sohail, L.Wang, B.Yamin, "Trust mechanism based AODV routing protocol for forward node authentication in mobile ad hoc network" in *Mobile Ad-hoc and Sensor Networks,* L. Zhu, S. Zhong, Eds. Beijing, China: Springer Singapore, 2018. pp. 338–349.

[30] C. Lee, U. Lee, M. Gerla, "Survey of Routing Protocols in Vehicular Ad Hoc Networks," in *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges,* M. Watfa Ed. Hershey PA 17033: IGI Global, 2015, vol. 9 (7), ch. 8, pp. 149-170.

[31] Y. Bai, Y. Mai, N. Wang, "Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs," in *2017 Wireless Telecommunications Symposium (WTS),* Chicago, IL, USA: IEEE, 2017, pp. 1-5.

[32] A. Kanthe, D. Simunic, R. Prasad, "Comparison of AODV and DSR on-demand routing protocols in mobile ad hoc networks," in *2012 1st International Conference on Emerging Technology Trends in Electronics, Communication & Networking,* Gujarat, India: IEEE, 2012, pp. 1-5, doi: 10.1109/ET2ECN.2012.6470118