International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V68I11P213
Volume 68 Issue 11, 97-104, November 2020

Multistage Security Detection in Mobile Ad-Hoc Network (MANET)

Muhannad Tahboush [1], Mary Agoyi [2], Abdllkader Esaid [3]

[1,3]*Department of Computer Engineering, Cyprus International University*

[2] *Information Technology Department, School of Applied Sciences, Cyprus International University*

Lefkosa- North Cyprus

[1]mh_tahboosh@yahoo.com

[2]magoyi@ciu.edu.tr

[3] aawatas2@gmail.com

Abstract *- Mobile Ad-hoc Networks (MANET) is a self-organized, non-centralized network of mobile nodes that communicate directly through intermediate nodes without infrastructure. MANET is vulnerable to several types of attacks and security threats, such as wormhole attacks. A wormhole attack captures the packets from one location of the network and tunnels them to another location to mislead the legitimate path and disrupt the network. Many algorithms based on round trip time (RTT) have been developed to overcome the wormhole attack. RTT is a message used to measure the distance in time perspective from source to all its neighbors. RTT suffers from many limitations such as processing delay, inaccurate value, and does not indicate any attack. This study proposes a Multistage Security Detection (MSD) algorithm based on RTT, PDR, and transmission. The Multistage security detection algorithm prevents a malicious node from taking over the legitimate path in MANET. MSD algorithm was implemented using an NS-2 network simulator. The performance metrics considered to evaluate the proposed algorithms and analyzing performance are delay, throughput, packet delivery ratio (PDR), packet dropping ratio, and the number of packets received. The proposed approach employs a popular reactive Ad-hoc On-Demand Distance Vector (AODV) routing protocol to enhance the detection method. MSD managed to outperform the previous study. The proposed detection algorithm (MSD) outperformed wormhole detection than the proposed algorithms in the literature.*

Keywords - *Wormhole attack. Malicious node. Legitimate node. AODV. MANET.*

I. INTRODUCTION

Mobile computing technology has been growing very quickly that has driven a revolution within the computing world. Mobile Ad-Hoc Network (MANET) consists of several mobile devices that wirelessly communicate with each other and operate directly within its radio coverage through task distribution without infrastructure or central base stations [1], [2]. Routing protocols such as AODV (Ad-hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing) are the wireless networks' backbone. They can show the best and shortest path between source and destination to achieve specific tasks. The MANET is an open medium, and the process of dynamic device communication whereby a node can enter or leave is simplified. This leads to changing network topology [3].

The network layers in MANETs are prone to several types of active attack and security threats, such as the black hole, Wormhole, Sybil, flooding, and Denial of Service (DoS) attacks [3]. Thus, it's important to ensure the confidentiality of data transmission in the wireless network from node to node without compromising data transmission integrity.

The wormhole attack is one of the gravest attacks and is challenging in detection. The wormhole attack process starts when an attacker captures the packet from one side of the network and sends the packet to the unauthorized side of the network to generate fake connections and mislead the legitimate path, which will result in packet loss, network disruption, affecting network routing and data aggregation [4], [5]. A wormhole attack does not need the knowledge of a security system, including cryptography mechanisms, public/private keys, etc. Thus even if a packet were encrypted with any encryption type, the malicious node would tunnel the packet to another distant malicious node [5].

A wormhole tunnel can be created as packets encapsulation (in-band) and out-of-band wormhole attack based on the medium used. In in-band attacks, the assailants will use the legitimate nodes that have been compromised and a valid existing wireless medium for building a link between malicious nodes to perform the attack, as shown in Fig.1. An in-band attack is very dangerous and does not need extra hardware to launch it.

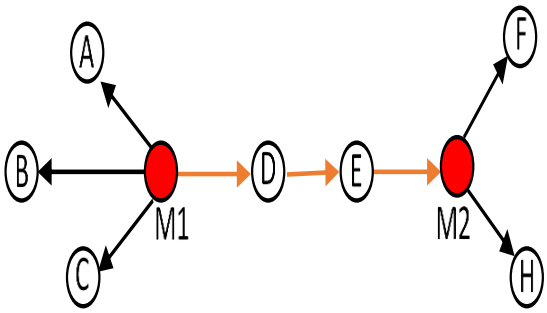


Fig.1 In-band wormhole attack between M1 and M2 nodes.

While an out-of-band attack can be established using a different wireless medium between two distant nodes to prevent the legitimate node from appearing, creating an illusion to the source that this link has the fewest number of hops and the destination is near. Therefore, high transmission mode and long-range directional wireless are required compared to the normal route to perform the attack [6], as illustrated in Fig. 2, which shows an out-of-band attack.

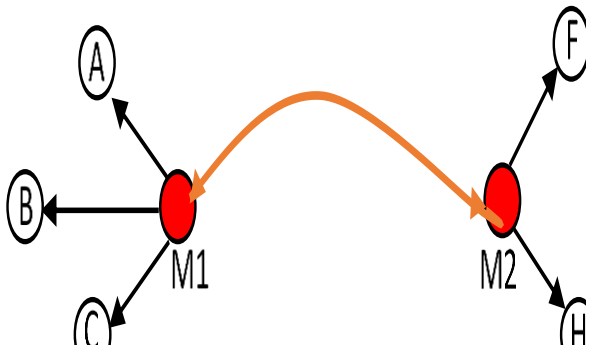


Fig.2 Out-of-band wormhole attack Between M1 and M2 nodes.

Although several studies have proposed Round Trip Time (RTT) to detect wormhole attacks, RTT is required by the packet to travel from the source to the destination and receive an acknowledgment. RTT provides location estimation, determines the nearest node to the source, and can determine the existence of malicious nodes most of the time. Relying on RTT alone would not be accurate enough during processing delays and for detecting short path wormhole. Besides, the adversary increases the number of neighboring nodes to increase the RTT value, generating an inaccurate RTT value that would prevent the malicious node's detection. [7], [8], [9] and [10].

While measuring PDR and transmission range alone will not suffice, the packet can be dropped due to a malicious node, a transmission error, or high traffic [8]. Malicious nodes also include themselves near the source node; in this case, the malicious node would be within the source's transmission range [11].

Due to the limitation of RTT of generating inaccurate values, an algorithm is proposed that will combine the advantages of RTT, PDR, and transmission range to achieve high detection accuracy of the wormhole attack. The proposed algorithm consists of three phases of detection methods for wormhole attack based on (AODV) protocol. These phases are manipulating transmission range, round trip time, and packet delivery ratio. The rest of this paper will be organized as follows. Section II provides the background. Section III overview of AODV protocol. Section IV shows the wormhole attack description and model. Section V shows the proposed methodology. Section VI provides an implementation. Section VII shows the analysis and results. Finally, section VIII, the conclusion.

II. BACKGROUND

Previous studies have proposed several methods and techniques to detect wormhole attacks in MANET.

As'adi et al. [12] proposed a modern decentralized mechanism for detecting a wormhole attack and malicious tunnels that is based on statistical metrics that utilize several new neighbor's nodes with an available number of neighbor's nodes for each node as its parameters to enhance the performance of the statistical wormhole apprehension network algorithm (SWAN). The authors applied some modifications to SWAN and then inserted these modifications as a secondary statistical disclosure parameter to it. The proposed mechanism detected wormhole attacks with low detection delay and did not create traffic overhead for routing protocol.

Sasirekha et al. [13] proposed an efficient and accurate scheme to detect and prevent sinkhole and wormhole attacks in MANET. The detection method was called the node collusion technique for assailant node detection. The available nodes will collude to determine the wormhole and sinkhole behavior, especially when the nodes suspect the attacker's existence in the path. Regarding the prevention of a malicious attack, they used the route a reserve method. The proposed schema will modify the AODV protocol with another routing protocol called Attack Aware Alert Ad hoc on-demand Distance Vector (A3AODV) that is more secure and able to alert the neighbor nodes against wormhole and sinkhole attacks.

Khobragade et al. [14] presented an efficient solution for detecting and preventing wormhole attacks in MANET called authentication-based delay per hop technique for Wireless Network. The proposed method used several hops and delays of each node in various directions in the network. The detection phase of wormhole attacks can be achieved by comparing the delay among hop and hop count information of different directions. The prevention phase utilizes the cryptography algorithm, known as Ceaser. This cipher checks node-id using some arithmetical processes that convert the input into ciphertext and vice versa at the receiver side to validate the legitimate node's signature.

Ahsan et al. [15] proposed a scheme for detection and mitigation of wormhole attacks that consist of two main methods of detection using Area Border Router (ABR) and Sensing Aware Nodes (SAN). The scheme will observe wireless nodes' signal strength, where the attack will be detected if the measured distance is higher than the default distance. To prevent the proposed scheme, fail down, there are two failsafe mechanisms. Designed in a way where one fails, the other will be immediately used instead to complete the system detection. Therefore, both the proposed schemes do not require any special hardware equipment, and both methods have a separate manner to promote comprehensive prevention and detection of system performance.

Majumder et al. [16] proposed an algorithm on Absolute Deviation (AD) of the statistical approach to preventing the wormhole attack. Both Absolute Deviation Covariance and Absolute Deviation Correlation work together to detect wormhole attacks at a rate no slower than other classical protocols. The node will be considered as a malicious node depending on the correlation coefficient. If the correlation coefficient between packets sent and received is high, it is considered a trusted node. Absolute Deviation techniques proved higher performance and required less time than AODV and measure the packet drop pattern for wormhole nodes using (ADCC) Absolute Deviation Correlation Coefficient.

Qazi et al. [17] proposed an efficient solution for wormhole detection and prevention, which consists of some modifications to the Delay per Hop Indicator (DelPHI) called (M-DelPHI) to operate in a multi-rate 802.11 wireless network since DelPHI does not provide security for AODV in a multi-rate wireless transmission. Three essential extensions have been proposed: multi-rate channel, Processing delay, and Neighbor monitoring. The new extension protocol (M-DelPHI) had been tested in various environments and perform higher protection than (DelPHI) against wormhole attacks for both in-band and out-of-band.

Teotia et al. [18] proposed a scheme called Cell-based Open Tunnel Avoidance (COTA) implemented on the location-aided routing protocol (LAR1) at network layers to perform route discovery operations instead of AODV protocol. The new method of combining both (COTA) and (LAR1) is called (COTA-LAR1). The outcomes from (COTA-LAR1) show the enhancement in routing schemes' security and protection against wormhole attacks in MANET in several metrics, such as PDR, end-to-end delay throughput.

Kaneria et al. [19] proposed a new algorithm called trusted AODV (TAODV) protocol, which employs hyperbolic tangent function to measure their neighboring nodes' trusted value. TADOV can enhance the system routine at each routing hop, such as trusted behaviors between all nodes, which will increase the opportunity to detect the node that exhibits malicious behavior. The outcomes show higher performance from TAODV than other standard AODV routing protocols.

III. OVERVIEW OF AODV PROTOCOL

Routing protocols are consisting of different types, reactive as well as proactive routing protocols. One of the popular reactive routing protocols is Ad-hoc On-demand Distance Vector (AODV) that is intended for use in wireless and mobile ad-hoc networks. AODV uses low energy and memory overhead while transmission. AODV supports both unicast and multicast routing, which employ when there is no valid route to the destination in the routing table. Therefore the source will generate on-demand route discovery processes and transmit a packet through various network nodes to the preferred destination. AODV employs four different types of messages, Route Request (REQ), Route Reply (RREP), Route Error (RERR), and hello (HELLO), to find and maintain the path to the destination [20]. Fig.3 shows the request RREQ message, and Fig.4 shows the RREP messages.

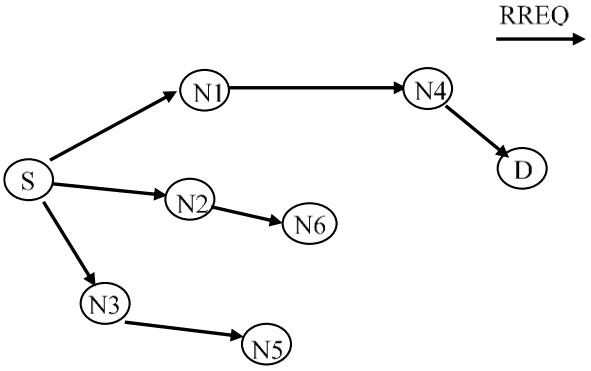


Fig.3 Route Request RREQ Process

In route request (RREQ) that support broadcast routing protocol, assume that S is the source and D is the destination. When the source is willing to send the packet to the destination and has no path to that destination in its routing table, the source will generate RREQ. The packet will be forwarded through intermediate nodes until reaching the appropriate destination D.

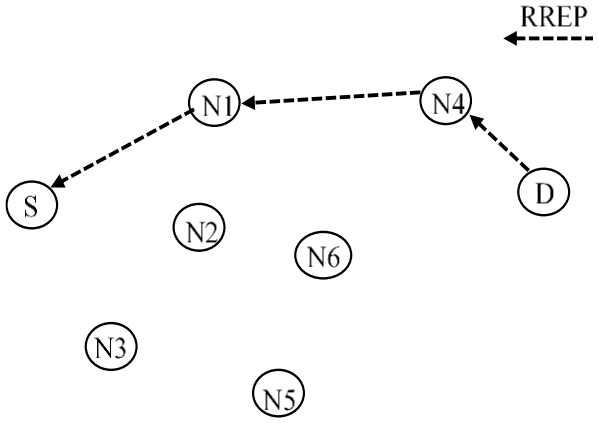


Fig.4 Route Reply RREP Process

The destination D will respond with an RREP (unicast routing) to the source S, which is a reverse path of the intermediate nodes (N4, N1) until the packet reaches S, the source in Fig.4.

IV. WORMHOLE ATTACK DESCRIPTION

A wormhole attack is one of the major attacks considered a challenging problem and can be launched at the OSI model's network layer. It consists of two or more malicious nodes involved in the routing path and the tunnel between them. The attacker eavesdropping and

record packets at one location in the network and transmit them to a different side or location in the network and then rebroadcasts the packet locally. As illustrated in Fig.5, the route between source *S* and destination *D* will be selected through the created tunnel *S, M1, M2, and D to form an out-of-band attack with fewer* hops. In contrast, the route is *S, M1, A, B, C, M2, D* forms an in-band attack [21] involved in the routing path through the legitimate nodes.

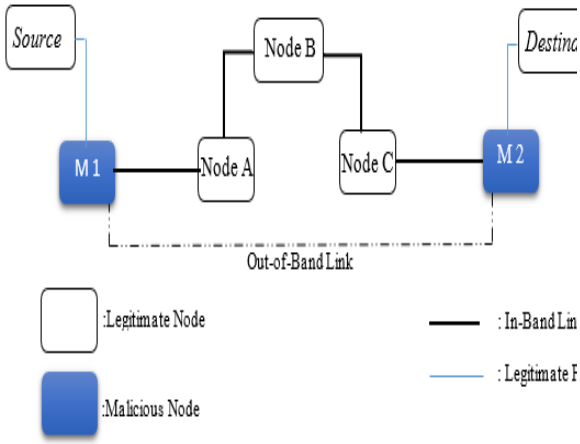


Fig.5 Wormhole attack between two malicious nodes

There are four types of tunnels, packet encapsulation, high power transmission, packet relay, and out-of-band, as mentioned in [22], [23]. This tunnel can be created by various connections such as wired and wireless transmission. The malicious nodes can exchange information between each other through the tunnel to form out-of-band or use encapsulate packets to launch in-band attacks. The packet will be forwarded through wormhole nodes by creating an illusion that they are close to each other when, in reality, they are not. Wormhole nodes are equipped with higher transmission power and higher bandwidth than legitimate nodes. Therefore, they can transmit packets over long distances to create fake shortcuts with many legitimate nodes in between, preventing the legitimate nodes from being discovered by its neighbors, creating incorrect routing paths, and then causing network disruptions [22], [24] and [25]. This fake shortcut link created by the wormhole node will be used for packet exchange among malicious nodes.

A. Wormhole Attack Model

There are three different categorizations of wormhole attacks: open Wormhole, half-open Wormhole, and closed Wormhole. In Open Wormhole: the assailants include themselves in the RREQ packet header in the route discovery process, where both nodes become part of the network to complete the communication path and prevent the legitimate nodes from being discovered by other nodes, changing the data integrity *(S, M1, M2, D)*. Half-Open Wormhole: the assailants are near the source and destination, where just one side of the malicious node can modify the data packet and the other side does not change it *(S, M1, D)*. Close Wormhole: a tunnel is created between two sides of the malicious nodes, and then rebroadcast the packet without any modification. The source and destination believe that they are close to each other in one hop *(S, D); Fig.* 6 shows wormhole models and routes. [26], [27].

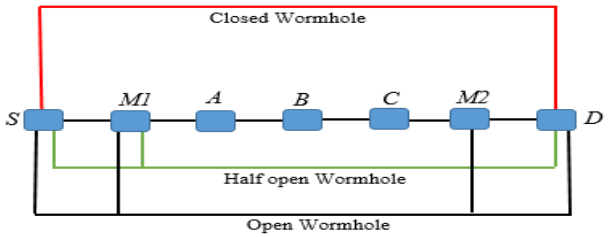


Fig.6 Wormhole Model

V. PROPOSED METHODOLOGY

In this paper, a Multistage Security detection (MSD) algorithm is proposed for wormhole attack detection in MANET. The main enhancement of the proposed protocol MSD is to build up a wormhole detection methodology that can prevent a malicious node from taking over the legitimate path during routing processes and data exchange without additional cost and equipment. Also, MSD can detect both in-band and out-of-band wormhole attack. MSD is based on the concept of three phases, round trip time (RTT), packet delivery ratio (PDR), and transmission range between two successive nodes.

The first phase is based on the transmission time that has been calculated between successive neighboring nodes to find out the transmission range. The neighboring node in the radio coverage (range) of the source node will be considered a legitimate node and pass to the RTT phase because legitimate nodes are close to one another and have limited radio coverage. Simultaneously, the link between every successive node having high transmission time would be considered an out-of-band wormhole. Transmission time between nodes can be calculated using intervals between Hello Packets, as shown in the equation (1) below.

$$\text{Hello Interval} = 2^{nd}\ \text{Hello\_Packet} - 1^{st}\ \text{Hello\_Packet} \quad (1)$$

The second phase is based on the RTT value, which is when the source nodes send the request and receive the reply message from the destination node. In this phase, the RTT value will be calculated to all immediate neighbors and comparing it to the threshold value. Because the RTT value between two fake neighbors is considered a higher value than two real neighbors, if the neighboring node's RTT value is lower than the threshold,

then the node will be assessed to the trusted list wormhole node that exists in that link. However, if the RTT value for that node is higher than the threshold, then a wormhole link may exist. Therefore the node will be added to the suspicious list and continue with the PDR phase. The threshold RTT value is determined by the equation (3) below:

Source node calculates the RTT using this formula:

$$\text{Total (RTT)} = \sum_{n=30}^{n=50} (n$$

Where *n* number of nodes
Calculate the threshold RTT by using this formula =

$$\text{Threshold RTT} = \frac{Total\ (RTT)}{n} \quad (3)$$

The third phase, where all nodes that reach this phase, will be examined by their packet delivery ratio (PDR), the number of packets received by the destination over the number of packets delivered by the source. The nodes in the suspicious list will be checked by PDR detection and compare their PDR with the threshold value selected using a deep neural network algorithm, where the input is all previous trace and mobility files (that resulted from the NS2 simulation). The algorithm processes the input one at a time and tries all possible values of the PDR, maintaining these results in their hidden units that implicitly contains information about the history of all the past PDR results. The output of the hidden units is the threshold value of the PDR to be compared with. If it's less than the threshold value, a wormhole node is detected in this route. Otherwise, that node is considered a trusted node, and no wormhole node exists in the link. Packet delivery ratio threshold is based on a neural network algorithm, as shown in Algorithm 1.

Packet delivery ratio can be measured using this formula:

$$\text{Packet Delivery Ratio} = \frac{\sum Number\ of\ packet\ received}{\sum Number\ of\ Packet\ Send} \quad (4)$$

Algorithm 1: PDR threshold value

1 *Run NS2* simulation
2 *Gather* the mobility, trace file, and result file that resulted from the previous simulation
3 *Run* the deep learning code
4 *Cluster* the input file for each node to be run as one element Else
5 *The algorithm* tries all possible values for PDR for Node A
6 *For* all results for Node A:
7 select *PDR* with the best results
8 The previous step is done for all nodes
9 Now, the *optimal PRD* for each node is ready
10 PDR for all nodes process to find the average optimal PDR for the network
End of Pseudocode.

Fig.7 PDR threshold algorithm

However, the three phases can detect and prevent wormhole attacks with high efficacy and performance. Each phase will achieve a particular detection such as transmission range, round trip time, and packet delivery ratio. The malicious node can be detected starting from the first phase of the detection phases. The proposed detection approach is performed by the nodes in the mobile ad-hoc network, as illustrated in algorithm 2.

Algorithm 2: MSD Proposed Detection Approach

```
1  Start
2  Nodes are deployed using the AODV protocol
3  RTT threshold is calculated
4  PDR threshold is calculated
5  Calculate the transmission time for each node in the routing table
     TT= Hello Packet 2 - Hello Packet 1
6  If (neighboring node in the range of source node) then
7        Start
8              If (RTT > threshold) then
9                 Add node to the suspicious list
10                      Start
11                            If (PDR>= threshold) then
12                                  Wormhole detected
13                            else
14                                  No wormhole attacks
15             else
16         No wormhole detected, add to the trusted table
17     else
18     Out of band detected
19 End of Pseudocode.
```

Fig.8 detection approach algorithm

VI. IMPLEMENTATION

The proposed algorithm (MSD) combines features of the three phases to provide high-performance detection for wormhole attacks. Firstly, it defines the network source and destination, as shown in Fig.9. The source node will select the best route to the appropriate destination based on the proposed algorithm. The number of nodes used in the proposed approach MSD starts from 30 nodes up to 50 nodes randomly deployed. The simulator increases 10 nodes for each successive scenario. The simulation will be done on each scenario to find out the result each time there is an increase of nodes in that scenario.

MSD has been measured by several metrics used to determine the performance of the proposed solution, such as the number of packet received, packet delivery ratio, throughput, packet dropping ratio, and delay. And the network performance has been analyzed and compared under a wormhole attack.

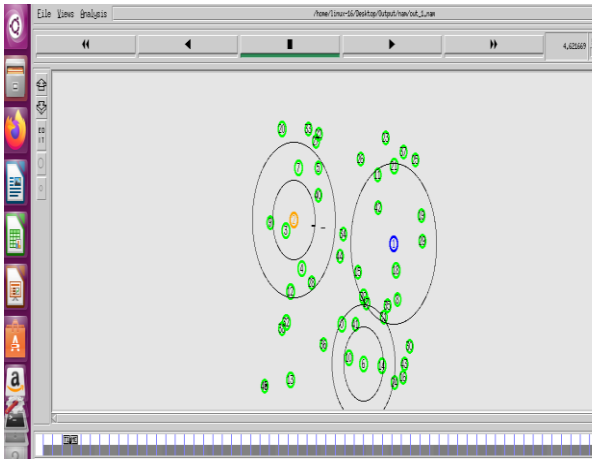


Fig.9 Scenario of sending a packet of 50 nodes

B. Network Assumption

To better introduce our proposed approach. The following network assumptions are considered in MSD.

1. All nodes are randomly distributed in a 2-dimensional square network.
2. All nodes use omnidirectional antennas for communicating with each other.
3. All nodes start with the same energy level.
4. The nodes have a random speed and mobility direction.
5. Two nodes are considered neighbors if the distance between them is within the transmission range.
6. When nodes are deployed, all nodes are legitimate nodes, and no malicious nodes are present.
7. It has been assumed that a malicious entity can launch many kinds of wormhole attacks.

VII. RESULT AND ANALYSIS

The performance of the proposed approach (MSD) is tested using the simulator NS-2.3 for a different number of nodes to measure many network metrics and compared with published results. A base article, Patel et al. [28], compares the obtained results with the proposed algorithm. The simulation network environment consists of nodes distributed randomly with a simulation parameter, as stated in table 1. The packet delivery ratio, throughput, end-to-end delay, and the number of dropping packets have been measured.

Parameter	Value
Simulator	NS-2.3
Operation System	Ubuntu 16.04 LTS
Topological area	1000 m x 1000 m
Simulation time	500 seconds
Node locations	Randomly
Radio propagation model	Two-ray ground reflection
Mobility model	Random waypoint
Traffic type	CBR
Packet size	512 bytes
Number of nodes	30,40 and 50 nodes
HELLO interval	milli-seconds (NS2 default)

A. No. of Packets Received

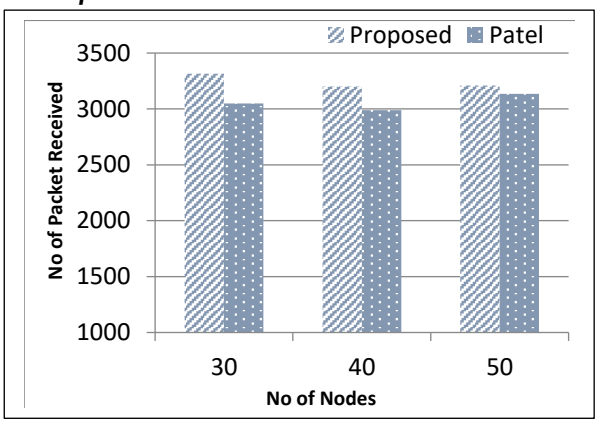


Fig.10 Comparison between Proposed MSD and Patel [28] for a packet received under wormhole attack

Fig.10 shows the data packet delivered from the source and received by the destination between Patel and proposed MSD through various node selection (30, 40, and 50). MSD approach can provide higher packet received than Patel because of delivery mechanism threshold that guaranty higher packets delivered which will reduce the number of dropping packet and mitigate the compromising packet during transmission, besides higher performance and throughput can be provided because it's directly proportional to the received packets over the Patel.

B. Packet Delivery Ratio

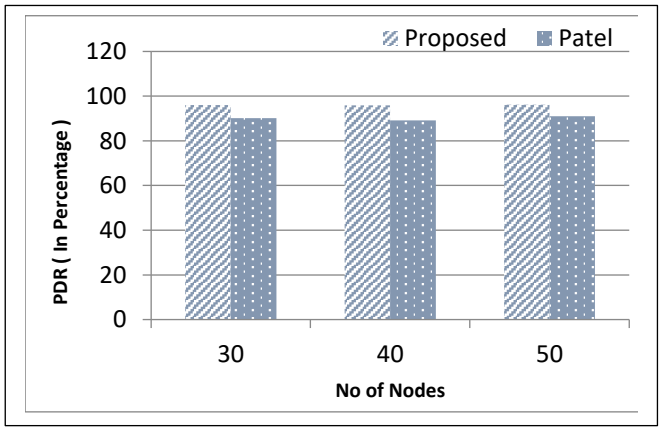


Fig.11 Comparison between Proposed MSD and Patel [28] for packet delivery ratio under wormhole attack

Fig.11 shows the improvement gained in MSD through packet delivery ratio and the efficiency of various network nodes (30, 40, and 50). The MSD proposed approach provides a higher packet delivery ratio value that is (96.1, 95.9, 96.2) respectively compared with Patel, which provides packet delivery ratio values (90.1, 89.1, 90.9)

respectively, due to the stability of the HWAD and provide lower delay that reduces the dropping packet for sending and receiving for both in-band and out-of-band wormholes. On the other hand, Patel has fewer PDR values because it rely on only RTT alone as a detection mechanism. Thus, MSD able to mitigate the attack while transmission occurs within the same area.

C. Throughput

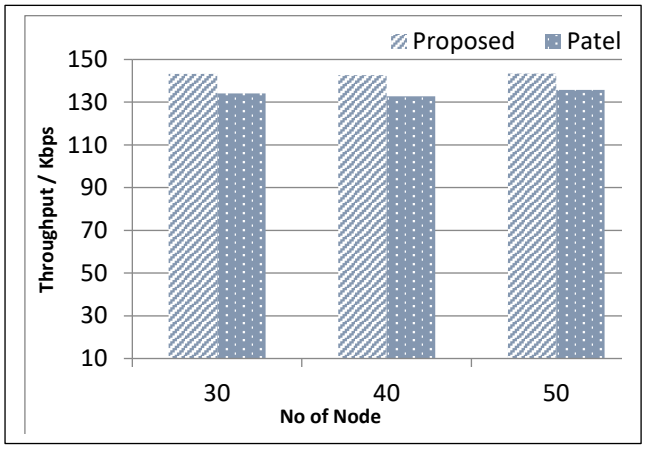


Fig.12 Comparison between Proposed MSD and Patel [28] for throughput under wormhole attack

Throughput can be defined by the amount of packet received at the destination at any given time and measured in (bps). As observed from Fig.12, the comparison between the MSD approach and Patel approach for throughput. The MSD proposed approach provides a higher throughput (143.2, 142.59, 143.4), respectively, compared with Patel (134.1, 132.7, 135.7). The MSD proposed approach can offer higher performance, quality, and successful throughput because lower delay provides related packet delivery to the destination. Patel approach that provides higher delay leads to lower throughput, especially at ode (50) provide (2.4 s).

D. Packet Dropping Ratio

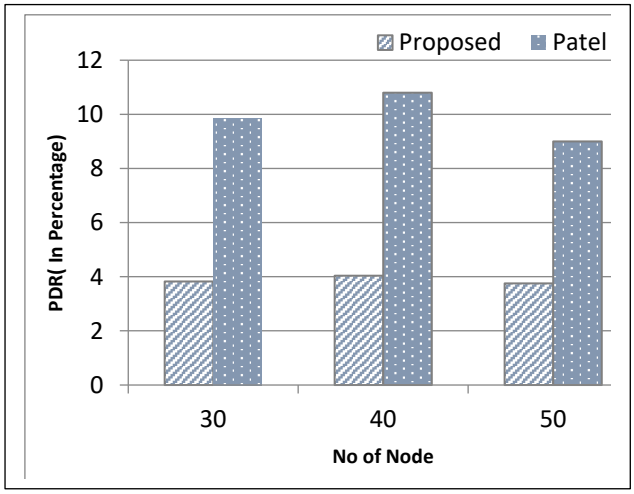
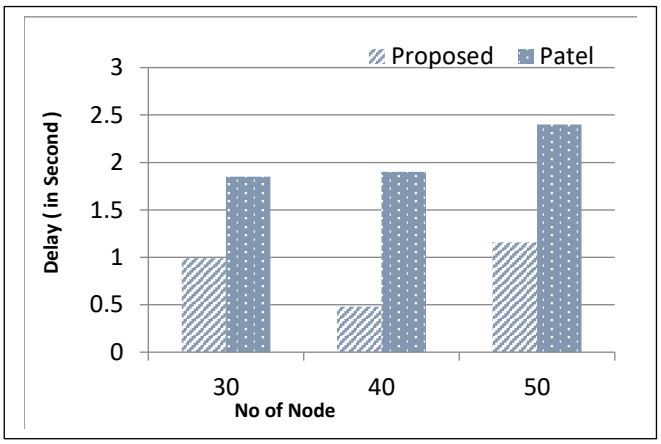


Fig.13 Comparison between Proposed MSD and Patel [28] for packet dropping ratio under wormhole attack

Fig.13 shows the number of packet dropping while transmitting data to the destination and the comparison between MSD proposed approaches and Patel approach. It has been realized that the proposed approach has a lower packet dropping along with a various number of nodes (30, 40, and 50) compare with the Patel approach. Therefore, the proposed approach can deliver the packets much better to the destination with higher performance and less congestion than the Patel approach, which has a higher packet dropping ratio, indicating high congestion and the waste of network resources.



E. Delay

Fig.14 Comparison between Proposed MSD and Patel [28] for delay under wormhole attack

Fig.14 shows the delay, which plays an important role in measuring network performance. The minimum delay leads to the highest data transmission to the destination and better quality of any network. Fig.14 introduces the comparison between the MSD approach and Patel in delay. The highest delay at node (50) that MSD approach reach is (1.2) second compare with the highest delay for Patel approach at the same network density reach (2.4) second due to the highest traffic and passing packets through a long tunnel in Patel Approach. MSD approach reduced the traffic and prevented creating a long tunnel by measuring the time between nodes. Therefore, the MSD approach's delay will take less time for packet transmitting and ensure the transmission's quality and performance.

VIII. CONCLUSION

MANET is the technology responsible for providing wireless data exchanging between mobile nodes. Thus, it's important to secure data packets while transmitting and preventing unauthorized users from accessing these data. In this paper, an algorithm is developed to enhance the wormhole attack detection on MANET called the Multistage security detection (MSD) algorithm in AODV.

The proposed detection uses the transmission range, round trip time (RTT), and packet delivery ratio. The MSD can detect both in-Band and out-of-band wormhole attacks The algorithm has been performed, and the experimental results demonstrated that the MSD has higher performance in various metrics. The proposed approach to wormhole detection has the potential to help wireless ad hoc networks improve security. Besides, MSD does not require any additional hardware equipment.

REFERENCES

[1] S. Majumder and D. Bhattacharyya, Mitigating wormhole attack in MANET using absolute deviation statistical approach, 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, (2018) 317-320.

[2] P. Sarkar, C. Kar, B. Sen, and K. Sharma, Sensitivity analysis on AODV with Wormhole attack, 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, (2016) 803-807.

[3] S. Amutha and K. Balasubramanian, Secured energy-optimized Ad hoc on-demand distance vector routing protocol, Computers and Electrical Engineering. 72 (2017).

[4] S. N. Ghormare, S. Sorte and S. S. Dorle, Detection and Prevention of Wormhole Attack in WiMAX Based Mobile Adhoc Network, 2018 Second International Conference on Electronics, Communication, and Aerospace Technology (ICECA), Coimbatore. (2018) 1097-1101.

[5] R. Singh, J. Singh, and R. Singh, WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks, 2016, Article ID 8354930. http://dx.doi.org/10.1155/2016/8354930.

[6] S. Eddie, B. Akbari, and P. Poshtiban, WANI: Wormhole avoidance using neighbor information, 7th Conference on Information and Knowledge Technology (IKT), Urmia, (2015) 1-6.

[7] S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay, and P. Kar, Wormhole Detection Based on Ordinal MDS Using RTT in Wireless Sensor Network, (2016) Article ID 3405264.

[8] R. Verma, R. Sharma, and U. Singh, New approach through detection and prevention of wormhole attack in MANET, International conference of Electronics, Communication, and Aerospace Technology (ICECA), Coimbatore. (2017) 526-531

[9] J. Anju and C. N. Sminesh, An Improved Clustering-Based Approach for Wormhole Attack Detection in MANET, 3rd International Conference on Eco-friendly Computing and Communication Systems, Mangalore. (2014) 149-154.

[10] A. Louazani, L. Sekhri and B. Kechar, A time Petri net model for wormhole attack detection in wireless sensor networks, International Conference on Smart Communications in Network Technologies (SaCoNeT), Paris. (2013) 1-6.

[11] W. A. Aliady and S. A. Al-Ahmadi, Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks, in IEEE Access, 7 (2019) 84132-84141.

[12] H. As'adi, A. Keshavarz-Haddad, and A. Jamshidi, A New Statistical Method for Wormhole Attack Detection in MANETs, 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Tehran. (2018) 1-6.

[13] D. Sasirekha and N. Radha, Secure and attack aware routing in mobile ad hoc networks against wormhole and sinkhole attacks, 2nd International Conference on Communication and Electronics Systems (ICCES), Coimbatore. (2017) 505-510

and provide more effective and accurate detection than Patel Approach.

[14] S. Khobragade and P. Padiya, Detection and prevention of Wormhole Attack Based on Delay Per-Hop Technique for Wireless Mobile Ad-hoc Network, International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi. (2016) 1332-1339.

[15] M. S. Ahsan, M. N. M. Bhutta and M. Maqsood, Wormhole attack detection in the routing protocol for low power lossy networks, International Conference on Information and Communication Technologies (ICICT), Karachi, (2017) 58-67.

[16] S. Majumder and D. Bhattacharyya, Mitigating wormhole attack in MANET using absolute deviation statistical approach, IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, (2018) 317-320.

[17] S. Qazi, R. Raad, Y. Mu, and Willy Susilo, Multirate DelPHI to secure multi-rate ad hoc networks against wormhole attacks, Journal of Information Security and Applications, (2018) 2214-2126.

[18] V. Teotia, S. K. Dhurandher, I. Woungang, and M. S. Obaidat, Wormhole prevention using COTA mechanism in position based environment over MANETs, IEEE International Conference on Communications (ICC), London, (2015) 7036-7040.

[19] P. Kaneria and A. Rajavat, Detecting and avoiding of wormhole attack on MANET using trusted AODV routing algorithm, Symposium on Colossal Data Analysis and Networking (CDAN), Indore. (2016) 1-5.

[20] A. M. El-Seminary and H. Diab, BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map, in IEEE Access. 7(2019) 95197-95211.

[21] P. Amish, V.B.Vaghela, Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol. 7th International Conference on Communication, Computing and Virtualization (2016).

[22] S. Deshmukh, S. Sonavane, A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things, The 12th International Conference Interdisciplinary in Engineering. (2019).

[23] M. Johnson, A. Siddiqui, and A. Karami, Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks, International Journal of Computer Applications (0975 - 8887) 174 (4) (2017).

[24] X. Luo et al., CREDND: A Novel Secure Neighbor Discovery Algorithm for Wormhole Attack, in IEEE Access, 7 (2019) 18194-18205.

[25] L. Lu, M. Hussain, G. Luo, and Z. Han, Pworm: Passive and Real-Time Wormhole Detection Scheme for WSNs, (2015), Article ID 356382.

[26] H. Shrivastava, S. Singh, A Survey on Wormhole Attack Detection in Wireless Network, (IJCSIT) International Journal of Computer Science and Information Technologies, 7(3) (2016) 1273-1276.

[27] R. Mudgal and R. Gupta, Study of various wormhole attack detection techniques in mobile ad hoc network, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai. (2016) 3748-3754.

[28] M. A. Patel and M. M. Patel, Wormhole Attack Detection in Wireless Sensor Network, International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore (2018) 269-274.