International Journal of Engineering & Technology, 7 (4) (2018) 3472-3477

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.15690
Research paper

Improved secure aware wormhole attack detection in mobile ad-hoc networks

Selladevi.M [1] *, Latha Maheswari.T [2], Duraisamy.S [3]

[1] *Research Scholar, Department of Computer Science, Chikkanna Govt., Arts College, Tirupur, Tamilnadu, India*
[2] *Assistant Professor, Department of Computer Application, Sri Krishna College of Engineering & Technology, Coimbatore, Tamilnadu, India*
[3] *Assistant Professor, Department of Computer Science, Chikkanna Govt., Arts College, Tirupur, Tamilnadu, India*
**Corresponding author E-mail: mschella30@gmail.com*

Abstract

The most challenging process in Mobile Ad-hoc Network (MANET) is detecting the wormhole attacks among various attacks. Most of the routing protocol doesn't have any defence mechanism against wormhole attacks and thus the presence of such attacks may disrupt the network communication by transmitting the packets to unknown location. Different routing protocols have been proposed for wormhole attack detection and prevention based on the different requirements like hardware, synchronization clocks, etc. To avoid such requirements, a Secure Wormhole Attack Detection (SWAD) technique was proposed based on the maximum end-to-end delay computation between two nodes within the transmission range. However, it does not consider the path length which is significantly reduced by the wormhole attacks. Hence in this article, Improved Secure Wormhole Attack Detection (ISWAD) technique is proposed. In this scheme, length of paths from source to any destination is calculated with the maximum end-to-end delay between nodes. Based on both computations, wormhole links through the network is detected and the data is transmitted via an alternative path available in the routing table. Finally, the simulation results show that proposed ISWAD technique achieves better performance than the existing technique in terms of different network metrics like throughput, jitter, etc.

Keywords: *End-To-End Delay; MANET; Path Length; Routing Protocol; Wormhole Attack Detection*.

1. Introduction

Particularly, a Mobile Ad-hoc Network (MANET) is a type of wireless network that consists of self-configuring mobile nodes which are moving independently in any direction within their communication range. This independent movement of the nodes cause frequent changes in network topology. The changes in network topology area complex challenge for several problems in MANET such as routing protocol, scalability and performance degradation [1-3]. Moreover, highly susceptible to different types of attacks like blackhole, grayhole, wormhole attacks, etc [4-5]. Among several attacks, wormhole attack detection is very difficult since the attacker does not require any break to launch this type of attack [6-8]. Wormhole attack [9] is the most dangerous attack against routing protocols in MANET where nodes attract the data packets from source at a particular location and retransmits them to the destination which locates at the other location by using a long range of link within the network [10]. It is a relay-based attack that can disrupt the routing protocol [11] and so network is disrupted or failed due to the reason of this attack. An attacker consists of two trusted nodes in two different locations of a network through a direct link between two nodes [12].The attacker records the packets at one location of a network and then tunnels the recorded packets to the different location. The attacker retransmits those packets back into the network location where it is coming from.

As a result, the entire routing is troubled. So, detection of wormhole attacks is very essential in MANET. This type of attack is classified into three types as open, closed and half-open wormhole attack [13]. Over the past decades, many researches have worked specifically on detecting wormhole attacks by using any special hardware, synchronization clocks, etc. Among different techniques, Delay Per Hop Indication (DelPHI) [14] was proposed to detect wormhole attacks by measuring delay of different paths to the destination from source. This technique requires neither synchronized clocks nor special hardware equipped mobile nodes for detecting wormhole attacks. Such requirements were avoided based on the novel Secure Wormhole Attack Detection (SWAD) technique [15]. This technique was performed by computing the maximum end-to-end delay between any two nodes within the communication range without any requirements to detect the wormhole attacks in the network. However, this technique has many limitations like it does not consider the length of paths passing through the wormhole attackers. Since, the path length can be reduced significantly while the attackers are presented in the selected routing path.

Hence in this article, Improved Secure Wormhole Attack Detection (ISWAD) technique is proposed that considers both path length and the maximum end-to-end delay for detecting the wormhole attacks through the MANET. The main aim of this technique is allowing a node to check whether a selected shortest path contains a wormhole tunnel or not. This proposed technique is achieved according to the fact that wormhole attacks reduce the paths from a source to a destination significantly, where the number of hops is very small compared to the normal path. Thus, the wormhole attack is efficiently detected by using both end-to-end delay and path length. If wormhole attacks through the network

are detected, then the path containing wormhole attacks will be removed from the routing table and data will transmit through alternative paths to the destination node.

The rest of the article is organized as follows: Section 2 gives an overview of related works. Section 3 presents the proposed wormhole attack detection technique. Section 4 illustrates the simulation results and Section 5 concludes the article.

2. Literature survey

Azer, M. A., et al. [16] proposed an innovative approach to detect and prevent wormhole attacks in wireless ad-hoc networks. This scheme was proposed based on the social science theory named diffusion of innovations and serves all network nodes during wormhole attack detection and prevention without prior interaction with malicious nodes. Moreover, the routing protocol was modified for allowing the path selection according to the node's opinions in each other's. This was achieved by facilitating each node for assigning weights to other nodes in the network via different phases. However, the end-to-end delay was increased.

Su, M. Y. [17] proposed a Wormhole Avoidance Routing Protocol (WARP) by anomaly detection in MANET. In this technique, a secure routing protocol was proposed based on Ad-hoc On-demand Distance Vector (AODV) protocol [18]. This proposed technique consists of link-disjoint multi-paths during route discovery and provides better route selection for avoiding malicious nodes. According to the characteristics, the wormhole nodes were simply removed from the routing path and the neighbors of wormhole nodes were enabled for discovering the wormhole nodes that have abnormal route interactions. After that, the wormhole nodes can be gradually isolated by their normal neighboring nodes. However, packet loss rate was high.

Shi, F., et al. [19] proposed time and location-based detection of wormhole attacks in wireless ad-hoc networks. In this scheme, two phases were involved such as detection phase and location phase. Based on the detection phase, the existence of wormhole attacks was detected and the wormhole nodes were identified in location phase. However, the performance efficiency was not improved.

Gupta, S., et al. [20] proposed a Wormhole attack detection protocol using Hound Packet (WHOP) in MANET. This technique was proposed without utilization of any special hardware like directional antenna and precise synchronized clock. Also, this protocol was independent of physical medium of wireless network and an additional hound packet was used for detection process. Once the path discovery process was completed, source node initiates wormhole attack detection process in the established route that counts hop difference between the neighbors of one hop away nodes in the path. Then, the wormhole was detected by the destination node if the hop difference between neighbors of the nodes was greater than the acceptable level. However, the detection speed of wormhole nodes was not improved.

Nayak, P., et al. [21] proposed wormhole attacks detection and prevention in MANET by using detection packet. In this technique, a general mechanism was proposed without the utilization of hardware, location information and clock synchronization. Here, detection packet was used for detecting malicious node in network which consists of three fields such as processing bit, count to reach next hop and time stamp. Timestamp was used for strongly detection with conformance at wormhole attack. Here, detection packet can simply be added in the wide range of ad hoc routing protocol for defending against wormhole attack. However, performance efficiency was less in terms of throughput, packet delivery ratio and end-to-end delay.

Chaurasia, U. K., & Singh, V. [22] proposed a wormhole attack detection using Modified AODV (MAODV) protocol. In this protocol, a wormhole attack was detected by using number of hops in different routes from source to destination. In addition, delay of each node in different paths was also used to detect the wormhole attacks in the network. By using such estimations, the destination node has the ability to detect the wormhole attack. However, this protocol was not efficiently worked while all the routes were wormhole affected.

Singh, Y., et al. [23] proposed a wormhole attack avoidance technique in MANET. The main objective of this technique was detecting the misbehaving nodes and preventing wormhole attack through the network by removing those nodes from the current routing paths and selecting the alternative path by path discovery process. This technique was proposed based on the modified Dynamic Source Routing (DSR) protocol [24] with the functionalities of wormhole attack detection and prevention. The message of wormhole node detection in the route was removed without affecting the overall network performance. This technique was used to detect such nodes and the paths that contain the misbehaving nodes were dropped and removed from the routing table of DSR. However, the throughput of this technique was less.

Kushwaha, D. S., et al. [25] proposed an efficient approach to detect and avoid wormhole attacks in wireless ad hoc networks. This technique does not require any requirements and used variations in routing information between neighbors for detecting wormholes. However, overall control packet and routing overhead were high. Biswas, J., et al. [26] proposed a Wormhole Attack Detection and Prevention (WADP) technique in MANET by using modified Ad hoc On-demand Distance Vector (AODV) routing protocol. In this technique, two additional fields in RREP packet were added that contains IP of intermediate node and unique number assigned to it. Here, the information of unique number was known only to authentic nodes. While a node was unable to specify the correct IP and number combination, it was treated as malicious. Moreover, node authentication i.e., a type of double verification was used for detecting malicious nodes and removing false positive issue that may arise in WADP algorithm. However, false positive issue was not removed when hidden wormhole attacks were launched.

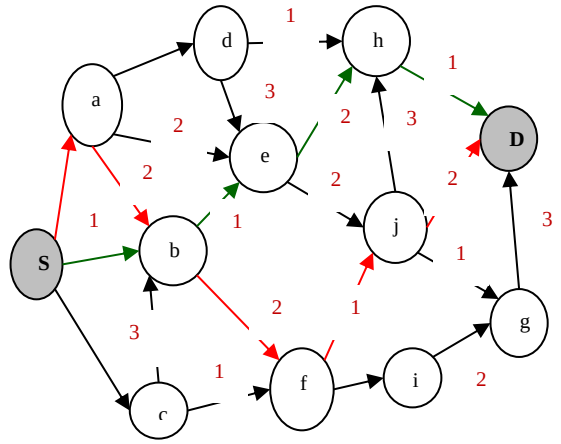
Giannetsos, T., & Dimitriou, T. [27] proposed a Localized and Delocalized Algorithm for Countering (LDAC) wormholes in MANET. Initially, the problem of neighbor discovery at physical and routing layer was studied. Then, a LDAC protocol was proposed to detect wormholes in both static and mobile wireless networks by enabling nodes for verifying the adjacency of a potential neighbor according to the connectivity information implied by the underlying communication graph. However, more effective protocol was required to improve the performance of wormhole attack detection.

3. Proposed methodology

In this section, the proposed Improved Secure Wormhole Attack Detection (ISWAD) is explained in brief. Consider the network which consists of mobile nodes and attackers. All nodes are homogeneous, symmetric and dynamic in nature. Common wireless communication range is used for establishing the transmission. In addition, consider each node have multiple neighbor nodes for constructing several disjoint paths. Consider that two wormhole nodes are linked with each other by using high speed connection called as out-of-band channel. Such long-range tunnel is known as wormhole link and two endpoints are called as wormhole nodes. The main aim of this proposed technique is detecting wormhole link with larger delay and reduced path length.

Figure 1 describes node h receives three RREQ packets; initially it is from first node d, so node h records this RREQ in its routing table as destination=S, next hop=D, hop count=3 and retransmits the RREQ. Then, it receives the similar RREQ from node e and records in its routing table as destination=S, next hop=e, hop count=3 and also drops the RREQ. Finally, node h receives another RREQ from the same source to the destination, it also records in its routing table as destination=S, next hop=j, hop count=4 and then drops it. All nodes execute the similar process until RREQ reaches the destination. When the destination receives the RREQ, it will initiate the process of detecting the wormhole attack. Here,

the packet transmission through the path "SabfjD" identifies as a wormhole link in the network. As a result, an alternative path such as "SbehD" will be chosen to transmit the data from source to destination.



S: Source Node

D: Destination Node

1-3: Arrival Sequence Number

Wormhole link

Alternative transmission path

Fig. 1: RREQ Receiving Process.

3.1. Computation of maximum end-to-end delay

The proposed technique utilizes AODV routing protocol for transmitting the data packets from source to destination. By using this protocol, the source node can endure a process for discovering the path to the destination. Thus, it transmits the packet to all of its neighbors. Initially, a source node transmits Route Request (RREQ) to the other nodes in its transmission range. When an intermediate node receives a RREQ, the node may analyse whether it exits in the routing table or not. Or else, it will create an entry in the routing table and retransmits the RREQ. When the number of hops is less than that exists in the routing table, it is replaced by the new next hop. Thus, the number of hops is replaced by the new number of hops. Here considers each node have a routing table with all routes to the destination, next hop and number of hops for reaching the source. Once the RREQ is received, an intermediate node will inform the source about the receive time of packet. By using the packet received time, the source node can examine the total time taken for packet transmission with one hop node. Then, the threshold for the maximum delay between two nodes is computed by source node. Also, the time difference between RREQ packet transmission and reception is computed whereas the maximum time difference i.e., end-to-end delay between source and its one hop neighbor is denoted as (T) and the threshold is defined as follows:

$$\text{Threshold} = T_{RREQ} + T_{RREP} + 2 * \left(T * \left((R_d/D) - 1\right)\right) \quad (1)$$

In equation (1), T_{RREQ} refers the time taken by the packet to reach the node, T_{RREP} refers the time taken by the packet to reach the source node during Route Reply (RREP) by its neighbor nodes, R_d refers the node's transmission range and D refers the distance between source and the neighbor which is computed as,

$$D = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (2)$$

In equation (2), (x_1, y_1) are coordinators of source node and (x_2, y_2) are coordinators of neighbor nodes. Based on this computation, the maximum end-to-end delay value is obtained between two nodes during RREQ packet transmission towards the destination which is shown in Figure 1 and forwarding RREP packet to the source node. The estimated threshold value is stored and compared with the time of each node during RREP packet reception from different paths. If the time difference between two nodes is larger than the threshold, then the wormhole link will be identified by the source node.

3.2. Computation of path length

To simplify the detection process, the path length is also computed including with the end-to-end delay. Here, Figure 1 is modeled as a graph to detect the worm link based on the computation of path length. Consider a graph $G(V, E)$where$V$is the set of vertices representing the nodes and E is a subset of $V \times V$. The elements of E are known edges representing the connections between the nodes. An edge is a pair of (i, j) of vertices which are boundaries of the edge. In this model, the path is considered as a sequence $(x_1, x_2, \ldots, x_k)$ of vertices such that there exists an edge between each pair of successive vertices in $G: \forall m, m = 1, \ldots, k-1 (x_m, x_{m+1}) \in E$. Consider $p_{x_1 x_k}$ is the set of paths of boundaries $x_1$andx_k,$p^y_{x_1 x_k}$ is the set of paths of boundaries x_1 and x_k passing through the node y,P is the set of paths defined on G. The path length is given by,

$$l: P \to N \quad (3)$$

$$p_{x_1 x_k} \mapsto l(p_{x_1 x_k}) = \text{Number of edges traversed by the path} = k - 1 \quad (4)$$

Consider x is a node belonging to V and the set of nodes located at the distance k from xis defined as,

$$S^k(x) = y, y \in V \text{ such as } D(x, y) = k \quad (5)$$

The one-neighbors of $x(S^1(x))$ is denoted as S(x). The malicious node is considered as a neighbor of the destination node (d)as,

$$x \text{ is malicious node} \Leftrightarrow x \in S(d) \quad (6)$$

During RREQ transmission at time T, a destination node can identify the wormhole node (wn) and request it to transit the routing table containing the list of neighbors S(wn). After that, the destination node establishes the set$S(d) \cap S(wn)$which is the set of neighbors of the destination and wormhole nodes. Consider the paths $p_s^{d,wn}$ and p_s^{wn} is defined as,

$$l(p_s) = \text{Inf}\{l(p); p \in p_s^x; x \in S(d) \cap S(wn)\} \quad (7)$$

$$l(p_s^{wn}) = \text{Inf}\{l(p); p \in p_s^{wn}\} \quad (8)$$

Here, p_s refers the shortest path obtained from neighboring nodes andp_s^{wn} refers the shortest path that passes through the wormhole node. The shortest path p_s^{wn} contains a wormhole link if and only if$\frac{l(p_s)}{l(p_s^{wn})} \geq \alpha$, where detection threshold $\alpha = 1.8$. Thus, wormhole attacks through the network are detected by comparing end-to-end delay and path length with the threshold value. Based on the both computations, the source node will not select that wormhole link and transmit the packet to the destination through the other communication link.

The step by step information of the proposed technique as follows:

1) The source node transmits RREQ to the other neighbor nodes.
2) Once RREQ is received, each neighbor nodes informs the source node about the time when the packet was received.

3) By using the packet received time, the source node can estimate the complete time taken for communicating with the neighbor nodes.
4) Source node can compute two detection threshold values for maximum delay between two nodes and path length from neighboring nodes.
5) Source node computes time difference between RREQ transmission time and RREQ receiving time based on the distanceD in which the maximum time difference is noted as maximum end-to-end delay(T).
6) According to the maximum end-to-end delay, source node can compute and store the threshold value as using (1) and (2).
7) The neighbor nodes forwards RREQ towards the destination and it will initiate RREP packets to the source node.
8) Source node can receive RREP packets via different paths which have different path lengths.
9) Each path length is computed by using (7) and (8) and compared with the other detection threshold value(α).
10) If both time difference and path length are greater the threshold values, then the wormhole link can be detected by the source node.
11) If wormhole links can be identified, then the source node will reject that path and transmit the data to the destination through the alternative path.

4. Results and discussion

In this section, the performance of the proposed ISWAD technique is compared with the existing SWAD, DelPHI technique by using Network Simulator (NS2.35). This evaluation is performed in terms of different network metrics such as throughput, end-to-end delay, jitter and packet delivery ratio. The simulation parameters are summarized in Table 1.

Table 1: Simulation Parameters

Simulation Parameters	Values
Simulation Tool	NS2.35
Channel Type	Wireless
Antenna Type	Omni Direction
Radio Propagation Model	Two Ray Ground
Simulation Area	1400×1400sqm
MAC Type	IEEE802.11
Frequency	914MHz
Number of Nodes	200
Transmission Range for Normal Network	250m
Transmission Range for Wormhole Network	500m
Mobility Model	Random Way Point
Node Velocity	10m/sec
Simulation Time	50sec
Packet Size	256bytes
Queue	Drop Tail
Queue Length	500
Pause Time	0.1m/sec
Traffic Type	TCP/CBR
Wormhole Link Length	1/2/3/4/5/6/7/8

4.1. Throughput

It defines the amount of packets successfully received by the destination in a given time. It is calculated as,

$$Throughput = \frac{Amount\ of\ packets\ correctly\ received\ by\ a\ destination}{Time\ taken} \quad (9)$$

Based on the highest throughput, the node's stability is improved and the number of wormhole attacks is reduced.

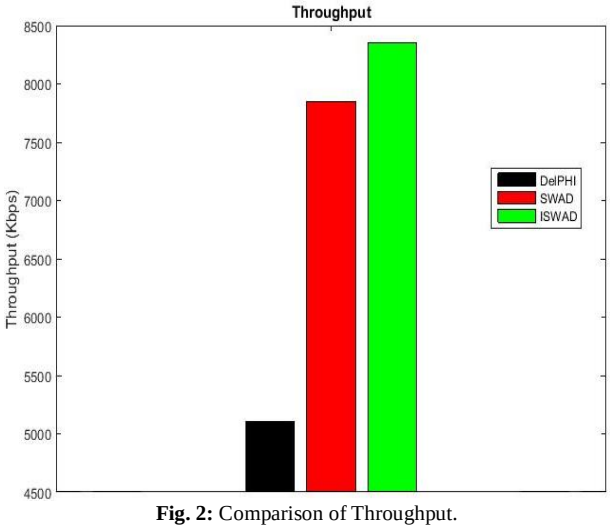


Fig. 2: Comparison of Throughput.

Figure 2 shows that the comparison of ISWAD with SWAD and DelPHI techniques in terms of throughput. It is analyzed that the throughput of ISWAD technique is 6.369% higher than SWAD technique and 63.73% higher than DelPHI technique. From the analysis, it is observed that the throughput of the ISWAD technique increases than the other techniques.

4.2. End-to-end delay

It refers the time taken to transmit the packets from source to destination. It is computed as,

$$Delay = \frac{Total\ time\ for\ packets\ received\ by\ the\ destination}{Total\ Number\ of\ packets\ received\ by\ the\ destination} \quad (10)$$

Delay is considered as one of the performance metrics which indicates that the network has less number of wormhole links while transmitting the packets from source to destination.

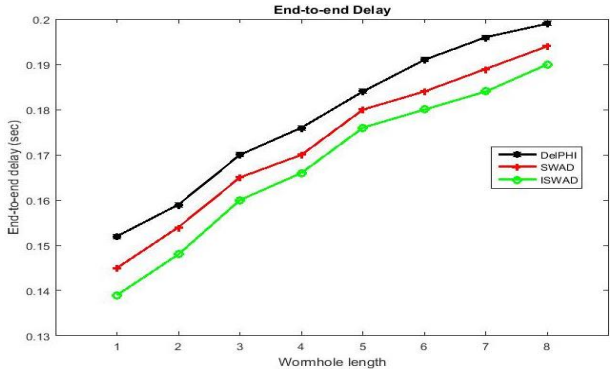


Fig. 3: Comparison of End-to-End Delay.

Figure 3 shows that the comparison of ISWAD, SWAD and DelPHI in terms of end-to-end delay according to the wormhole link length. It is analyzed that the end-to-end delay of ISWAD is 2.577% less than SWAD and 4.523% decreased than DelPHI technique when wormhole link length is considered as 8. From the analysis, it is observed that the end-to-end delay of the proposed ISWAD technique decreases in according to the varying wormhole link length than the existing techniques.

4.3. Jitter

It is defined as the variation in the delay of received packets. It is used to identify the number of packet loss through the network.

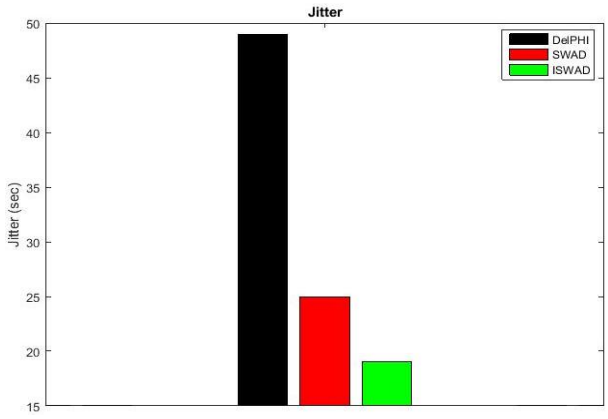


Fig. 4: Comparison of Jitter.

Figure 4 shows that the comparison of ISWAD with existing SWAD and DelPHI in terms of jitter. It is analyzed that the jitter of ISWAD is 24% less than SWAD technique and 61.224% reduced than DelPHI technique. From the analysis, it is observed that the jitter of the ISWAD technique decreases than the other existing techniques.

4.4. Packet delivery ratio

It refers the percentage of total number of packets received by the destination to the total number of packets transmitted from the source. It is computed as,

$$Packet\ Delivery\ Ratio = \frac{Total\ number\ of\ packets\ received\ by\ destination}{Total\ number\ of\ packets\ transmitted\ by\ source} \times 100 \quad (11)$$

According to the high PDR, the packets are sent to the destination without any wormhole attacks through the network.

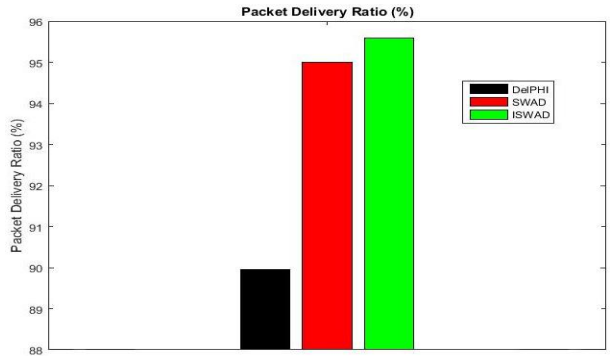


Fig. 5: Comparison of Packet Delivery Ratio.

Figure 5 shows that the comparison of proposed and existing techniques such as ISWAD, SWAD and DelPHI in terms of packet delivery ratio. It is analyzed that the packet delivery ratio of ISWAD technique is 0.589% higher than SWAD technique and 6.237% higher than DelPHI technique. From the analysis, it is observed that the packet delivery ratio of the ISWAD technique increases than the other techniques.

5. Conclusion

In this article, Improved Secure Wormhole Attack Detection (ISWAD) technique is proposed for improving the wormhole attack detection in the MANET. This proposed technique does not require any requirements to detect the wormhole attacks. The proposed technique utilizes two threshold values to identify the wormhole link by comparing those values with the end-to-end delay between two nodes and the path length of suspected node i.e., wormhole node. If the suspected node has high end-to-end delay and less path length, then the source node can detect the wormhole link through the network. Finally, the simulation results prove that the proposed ISWAD technique has the highest ability to detect all wormhole links than the existing technique and achieves better performance in terms of throughput, end-to-end delay, etc. In future, system parameters like node density, wormhole range, etc., would be considered to detect wormhole attacks efficiently.

References

[1] Kumar M, & Mishra R (2012), "An overview of MANET: history, challenges and applications", *Indian Journal of Computer Science and Engineering*, *3*(1), pp. 121-125.

[2] Goyal P, Parmar V, & Rishi R (2011), "Manet: vulnerabilities, challenges, attacks, application", *IJCEM International Journal of Computational Engineering & Management*, *11*(2011), pp. 32-37.

[3] Raghavendran CHV, Satish GN, & Varma PS (2013), "Security challenges and attacks in mobile ad hoc networks", *I.J. Information Engineering and Electronic Business*, *3*, pp. 49-58. https://doi.org/10.5815/ijieeb.2013.03.06.

[4] Reddy PN, Vishnuvardhan CH, & Ramesh V (2013), "Routing attacks in mobile adhoc networks", *International Journal of Computer Science and Mobile Computing*, *2*(5), pp. 360-367.

[5] Kaushal S, & Aggarwal R (2015), "A study of different types of attacks in MANET and performance analysis of AODV protocol against wormhole attack", *International Journal of Advanced Research in Computer Engineering & Technology*, *4*(2), pp. 301-305.

[6] Nivedha S, & Narayanan SS (2015), "Detection and prevention of wormhole attack in MANET using new fresh algorithm", *International Journal of Advanced Research in Computer Engineering & Technology*, *4*(5), pp. 2321-2326.

[7] Maulik R, & Chaki N (2011), "A study on wormhole attacks in MANET", *International Journal of Computer Information Systems and Industrial Management Applications*, *3*, pp. 271-279.

[8] Thalor J, & Monika M (2013), "Wormhole attack detection and prevention technique in mobile ad hoc networks: a review", *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(2), pp. 137-142.

[9] Awad B, & Barhoom T (2015), "BT-WAP: Wormhole Attack Prevention Model in MANET Based on Hop-Count", *Network*, *4*(7), pp. 600-606.

[10] Shrivastava H, & Singh SP (2016), "A survey on wormhole attack detection in wireless network", *International Journal of Computer Science and Information Technologies*, *7*(3), pp. 1273-1276.

[11] Sharma N, & Singh U (2014), "Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks", *International Journal of Computer Science and Mobile Computing*, *3*(2), pp. 29-33.

[12] Enshaei M, & Hanapi ZB (2015), "A review on wormhole attacks in MANET", *Journal of Theoretical and Applied Information Technology*, *79*(1), pp. 7-21.

[13] Kaur M, & Kalra S (2016), "A survey on wormhole attack detection and prevention techniques in mobile adhoc networks", *International Journal of Scope of Computer Research*, *5*(4), pp. 038-042.

[14] Arora SK, & Ayushree (2016), "Detection and Performance Analysis of Wormhole Attack in MANET using DELPHI Technique", *International Journal of Security and Its Applications*, *10*(10), pp. 321-330. https://doi.org/10.14257/ijsia.2016.10.10.28.

[15] Kaur P, Kaur D, & Mahajan R (2017), "Wormhole Attack Detection Technique in Mobile Ad Hoc Networks", *Wireless Personal Communications*, *97*(2), pp. 2939-2950. https://doi.org/10.1007/s11277-017-4643-z.

[16] Azer MA, El-Kassas SM, & El-Soudani MS (2010), "An innovative approach for the wormhole attack detection and prevention in wireless ad hoc networks", In *IEEE 2010 International Conference on Networking, Sensing and Control (ICNSC)*, pp. 366-371. https://doi.org/10.1109/ICNSC.2010.5461523.

[17] Su MY (2010), "WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks", *Computers & Security*, *29*(2), pp. 208-224. https://doi.org/10.1016/j.cose.2009.09.005.

[18] Maurya PK, Sharma G, Sahu V, Roberts A, & Srivastava M (2012), "An overview of AODV routing protocol", *International Journal of Modern Engineering Research*, *2*(3), pp. 728-732.

[19] Shi F, Jin D, Liu W, & Song J (2011), "Time-based detection and location of wormhole attacks in wireless ad hoc networks", In *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1721-1726.

[20] Gupta S, Kar S, & Dharmaraja S (2011), "WHOP: Wormhole attack detection protocol using hound packet", In *IEEE 2011 international conference on Innovations in information technology (IIT)*, pp. 226-231. https://doi.org/10.1109/INNOVATIONS.2011.5893822.

[21] Nayak P, Sahay A, & Pandey Y (2013), "Detection and prevention of wormhole attacks in Manets using detection packet", *International Journal of Scientific & Engineering Research*, *4*(6), pp. 1216-1222.

[22] Chaurasia UK, & Singh V (2013), "MAODV: Modified wormhole detection AODV protocol", In *IEEE 2013 Sixth International Conference on Contemporary Computing (IC3)*, pp. 239-243. https://doi.org/10.1109/IC3.2013.6612197.

[23] Singh Y, Khatkar A, Rani P, & Barak DD (2013), "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks", In *IEEE 2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT)*, pp. 283-287. https://doi.org/10.1109/ACCT.2013.68.

[24] Poonia R, Sanghi AK, & Singh D (2011), "DSR routing protocol in wireless ad-hoc networks: Drop analysis", *International Journal of Computer Applications*, *14*(7), pp. 18-21. https://doi.org/10.5120/1896-2527.

[25] Kushwaha DS, Singh VK, Singh S, & Sharma S (2014), "An efficient approach for detecting and avoiding wormhole attacks in wireless ad hoc networks", *International Journal of Advances in Electronics and Computer Science, 1*(2), pp. 39-43.

[26] Biswas J, Gupta A, & Singh D (2014), "WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol", In *IEEE 2014 9th International Conference on Industrial and Information Systems (ICIIS)*, pp. 1-6. https://doi.org/10.1109/ICIINFS.2014.7036535.

[27] Giannetsos T, & Dimitriou T (2014), "LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks", *Journal of Computer and System Sciences*, *80*(3), pp. 618-643. https://doi.org/10.1016/j.jcss.2013.06.015.