International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Artificial Immune System Based Improved Secure-Aware Wormhole Attack Detection in MANET

M. Selladevi, T. Lathamaheswari, S. Duraisamy

Abstract*: Typically, the most significant challenge in Mobile Adhoc Network (MANET) is detecting the wormhole attacks in the network during communication that degrades the overall network performance. Many routing protocols have been developed to detect and prevent the wormhole attacks based on the requirements of hardware, synchronization clocks, etc. To avoid those requirements, Improved Secure-aware Wormhole Attack Detection (ISWAD) technique was proposed by considering the maximum end-to-end delay and path length from source to the destination node. However, it requires more parameters to further increase the detection accuracy. Therefore in this article, an Artificial Immune System (AIS) based ISWAD is proposed to detect the wormhole attacks efficiently. Initially, a scalable and distributed scheme is applied to avoid single point failures and high mobility by using the sequential probability ratio test. In this scheme, system parameters are also considered with the maximum end-to-end delay and path length. To further improve the detection rate, these parameters are learned by the AIS to detect the wormhole attacks through the network precisely. After the wormhole links/nodes are detected, an alternative path is chosen from the routing table to transmit the data from source to the destination without any packet loss. Finally, the simulation results demonstrate that the proposed technique achieves better detection rate than the other wormhole attack detection techniques.

***Index Terms*: MANET, Wormhole attack detection, ISWAD, Scalable and distributed scheme, Artificial immune system**

I. INTRODUCTION

A Mobile Adhoc Network also known as 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 causes frequent changes in network topology. The changes in net-work topology area complex challenge for several problems in MANET such as routing protocol, scalability and performance degradation [1]. Moreover, highly susceptible to different types of attacks like blackhole, grayhole, wormhole attacks, etc [2]. Among several attacks, wormhole attack detection is very difficult since the attacker does not require any break to launch this type of attack [3].

Wormhole attack [4] 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. It is a relay-based attack that can disrupt the routing protocol 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. 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.

In previous researches, a novel Secure Wormhole Attack Detection (SWAD) technique [5] was proposed 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. As a result, an Improved Secure Wormhole Attack Detection (ISWAD) [6] technique was proposed that considers both path length and the maximum end-to-end delay to detect the wormhole attacks in the network. However, it requires more parameters to further improve the detection accuracy.

Hence in this article, AIS-based wormhole attack detection is proposed in MANET. In this technique, a scalable and distributed analysis is introduced that uses sequential probability ratio test to detect single point failure and control high mobility of the nodes. Here, the system parameters such as false positive, false negative, detection time variation, node density, system overhead, storage aspects and wormhole range on attacker's risk are determined to improve the detection accuracy.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
M. SellaDevi*, Department of Computer Science, Chikkanna Govt., Arts College, Tirupur, Tamilnadu, India.
T. Lathamaheswari, Department of Computer Application, Sri Krishna College of Engineering & Technology, Coimbatore, Tamilnadu, India.
S. Duraisamy, Department of Computer Science, Chikkanna Govt., Arts College, Tirupur, Tamilnadu, India.

Further, the obtained parameters are learned by using AIS algorithm to detect the wormhole attacks through the network. Based on this learning-based wormhole attack detection, the detection speed and accuracy are improved significantly.

The rest of the article is organized as follows: Section II presents the works which is related to the wormhole attack detection in MANET. Section III explains the concept about the proposed wormhole attack detection mechanism. Section IV describes the performance evaluation of the proposed mechanism. Finally, Section V concludes the research work

II. LITERATURE SURVEY

Wormhole attack detection [7] was proposed for preventing adhoc networks routing protocols. In this approach, two phase process was proposed by one or more malicious nodes. Initially, the malicious nodes called wormhole nodes were used for baiting legitimate nodes in order to transmit the data to the other nodes through them. Then, the wormhole nodes may perhaps exploit the data in different ways. Moreover, the wormhole attack nodes from an attacker's perspective were analyzed and new improvements on this type of attacks were also suggested.

Time and location-based detection of wormhole attacks [8] was proposed in wireless adhoc 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.

A Wormhole attack detection protocol [9] was proposed by 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.

Wormhole attacks detection and prevention scheme [10] was proposed in MANET based on the packet detection. In this technique, 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 adhoc routing protocol for defending against wormhole attack. However, performance efficiency was less in terms of throughput, packet delivery ratio and end-to-end delay.

Wormhole attack detection [11] was proposed by using a 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.

A Localized and Delocalized Algorithm was proposed for Countering (LDAC) wormholes [12] in MANET. Initially, the problem of neighbor discovery at physical and routing layer was studied. Then, a LDAC protocol was pro-posed to detect wormholes in both static and mobile wireless net-works 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.

A Wormhole Resistant Hybrid Technique (WRHT) [13] was proposed in Wireless Sensor Network (WSN) based on the concept of watchdog and Delphi schemes to guarantee the wormhole will not be left untreated in the sensor network. In this technique, the dual wormhole detection mechanism was used for computing the probability of factor time delay and packet loss probability of the established path in order to find the probability value of wormhole presence. However, the performance efficiency was not analyzed in terms of throughput, end-to-end delay and other parameters.

Wormhole attack prevention and detection using authentication based delay per hop technique [14] was proposed for wireless ad-hoc network. In this technique, the detection of wormhole was achieved by using number of hops and delay of each node in different routes available in the network. The sender node has the ability to detect the wormhole attacks. However, the performance was not analyzed efficiently.

Jitter Monitoring based wormhole attack detection, namely JITWORM [15] was proposed in MANET to detect the wormholes with variable delay. In this technique, the wormhole attack during path discovery and data transmission phases was detected by employing a mechanism of analyzing the jitter applied to packets by the nodes. Each node monitors the jitter applied to packets by its neighboring nodes. After successful detection of a wormhole, it can be isolated from the network. However, it requires wormhole detection during RREP phase by analyzing the link quality.

An efficient and reliable methodology [16] was proposed for wormhole attack detection in WSN. In this methodology, an efficient and reliable wormhole attack detection and localization based scheme was proposed to minimize the detection cost of wormhole attacks on the basis of key observation that a large number of network traffic was concerned by the wormholes. However, this scheme has high energy consumption and simulation time.

A computationally intelligent approach [17] was proposed for detecting the wormhole attacks in WSN. In this approach, Artificial Neural Network (ANN) was proposed to detect the probable locations of the wormhole nodes in both uniformly and non-uniformly distributed sensor networks.

However, an accurate location of the malicious nodes was not identified.

III. PROPOSED METHODOLOGY

In this section, the proposed AIS-ISWAD technique is explained briefly. Initially, the network is considered with the number of mobile nodes and attackers. Each node is homogeneous, symmetric and dynamic in nature. The data transmission between source and destination is established by using a common wireless communication range. Additionally, each node has many neighboring nodes in order to construct the different disjoint paths. Assume that two wormhole nodes are connected with each other by using an out-of-band channel. Such long-range tunnel between two endpoints i.e., wormhole nodes is called as wormhole link. The major goal of this proposed technique is reducing the computational time of wormhole attack detection based on the learning process and improving the detection rate by considering the different system parameters. The flow diagram of this technique is shown in Figure 1.

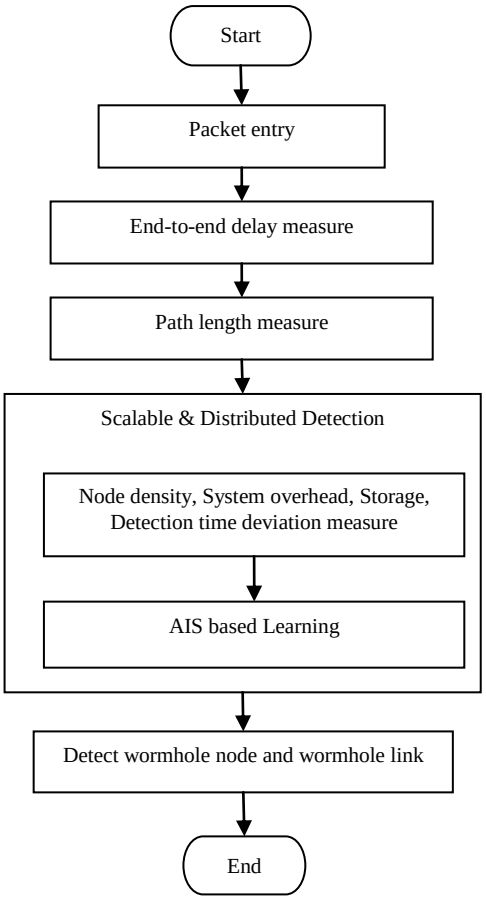

Fig.1: Flow Diagram of AIS-ISWAD Technique

A. Sequential Probability Ratio Test (SPRT) for Wormhole Detection

This technique was proposed based on the events generated by the nodes which are given as samples to the respective decision engines to make decisions on paths having wormhole links. Each node maintains the routing table that stores the next hop node to which the packet should be transmitted to reach the specific destination node. Anode (u)generates an event such as C (change) or UC(un-change)event for each destination node(v)regularly after every Ψsecond.These events are transmitted to the decision engine in $u$for making a decision as whether the path contains a wormhole link or not.Consider $P(u,v)$ is the path between nodes $u$and v. Each C event generated by node u for v reduces the value of the decision variable$D_{u,v}$supporting the hypothesis that$P(u,v)$ does not have the wormhole links.AnUC event increases the value of $D_{u,v}$ supporting the hypothesis that $P(u,v)$has at least one wormhole link.

Consider two hypotheses H_1 and H_0 where H_1 indicates the hypothesis that the path to a given node is attacked andH_0indicates the hypothesis that the path to a given node is not attacked. Assume $D_m^{u,v}$ is the evaluation of $P(u,v)$ by node u after receiving the event x_m and$D_{u,v}$ is the value of the most recent evaluation. When an event x_m for node $v$is generated by the node u, the value of $D_m^{u,v}$ is computed by the decision engine of node u as follows:

$$D_m^{u,v} = \begin{cases} D_{m-1}^{u,v} e \times \frac{P(C|H_1)}{P(C|H_0)} & if\ x_m = C \\ D_{m-1}^{u,v} \times \frac{P(UC|H_1)}{P(UC|H_0)} & if\ x_m = UC \end{cases} \quad (1)$$

Where $D_0^{u,v} = 1$

Here, two threshold values U and V are introduced to define how suitably large or small D_m must be chosen for decision making. If$D_m \geq U$, then H_1 is true i.e., the path $P(u,v)$ is attacked and if$D_m \leq V$, then H_0 is true i.e., the path $P(u,v)$ is not attacked. If $V < D_m < U$, then an additional iteration with a new event x_{m+1} will prepared. These threshold values should be selected carefully for minimizing the error during decision making process. As a result, system parameters α_1 and α_2 where α_1 refers the false positives, α_2 is the false negatives are used. Therefore, the values of U and V are bounded by $U \leq (1-\alpha_2)/\alpha_1$ and $V \geq \alpha_2/(1-\alpha_1)$ correspondingly and the test provides a sufficient accuracy if the values of U and V are selected as $(1-\alpha_2)/\alpha_1$ and $\alpha_2/(1-\alpha_1)$ respectively.

The conditional probabilities $P(C|H_1), P(C|H_0), P(UC|H_1)$ and $P(UC|H_0)$ are depending on the conditional probabilities $P_{wormhole}$ and $P_{legitimate}$of an UCevent being generated by a path which is free from the wormhole links and an UC event being generated by a path having wormhole links, respectively.

$$P(C|H_1) = 1 - P_{wormhole} \quad (2)$$
$$P(C|H_0) = 1 - P_{legitimate} \quad (3)$$
$$P(UC|H_1) = P_{wormhole} \quad (4)$$
$$P(UC|H_0) = P_{legitimate} \quad (5)$$

Moreover, an optimum time period Ψ is computed to generate the events by u for all destinations which have paths via $v$from u. Assume M^u and M^v are the vectors representing the nobilities of the nodes u and v respectively and split by an inner angle θ in the range[0,180]. The relative mobility $M^{u,v}$ is computed as follows:

$$M^{u,v} = |M^u - (M^u \times \cos\theta)| \quad (6)$$

Here, $(M^u \times \cos\theta)$ gives the component of M^valongM^u. It is considered that all nodes can move with the same mobility M in random directions and the relative mobility $M^{u,v}$ is defined as:

$$M^{u,v} = M(1-\cos\theta) \quad (7)$$

If d_{avg} is the average distance between the neighbors while nodes are located randomly, then Ψ is computed as follows:

$$\Psi = \frac{R_{node}-d_{avg}}{M^{u,v}} \quad (8)$$

$$\text{Where } d_{avg} = \frac{R_{node}}{\sqrt{2}} \quad (9)$$

In equation (8), R_{node} refers the transmitting range of a node's transmitter and the above equation (8) can be rewritten by using (7) and (9) as:

$$\Psi = \frac{R_{node}(\sqrt{2}-1)}{\sqrt{2}M(1-\cos\theta)} \quad (10)$$

Additionally, the values of $P_{wormhole}$ and $P_{legitimate}$ are computed to update the value of the decision variable. The conditional probability that legitimate paths generate an UC event iscomputed by,

$$P_{legitimate} = \frac{M(1-\cos\theta)}{2M} = \frac{1-\cos\theta}{2} \quad (11)$$

Here, the component $2M$ indicates the maximum relative mobility while the nodes u and v move in the opposite direction i.e., when $\theta = 180$. The value of $P_{legitimate}$ is reduced by reducing the value of θ.Similarly, $P_{wormhole}$ refers the conditional probability that an UC event is generated by a path having at least one wormhole link. This is due to the transmitting range of$R_{wormhole}$ of a wormhole is high compared to the transmitting range of R_{node} of a node. Therefore, most of the nodes can remain within $R_{wormhole}$and so an UC event is generated.

For an C event to be produced after Ψ second, a neighbor v should navigate a larger distance by moving with a high mobility(M'^{v}), resulting in higher relative mobility$M'^{(u,v)}$with respect to the decision making node u and the value of $M'^{(u,v)}$ is computed as:

$$M'^{(u,v)} = \frac{R_{wormhole}(\sqrt{2}-1)}{\sqrt{2}\Psi} \quad (12)$$

By considering the inner angle of split between mobility vectors M^{u} and M'^{v} as θ', the above equation (12) can be rewritten as follows:

$$\Psi = \frac{R_{wormhole}(\sqrt{2}-1)}{\sqrt{2}M(1-\cos\theta')} \quad (13)$$

The equations (10) and (13) are equated as:

$$\frac{R_{wormhole}(\sqrt{2}-1)}{\sqrt{2}M(1-\cos\theta')} = \frac{R_{node}(\sqrt{2}-1)}{\sqrt{2}M(1-\cos\theta)} \quad (14)$$

$$1-\cos\theta' = \frac{R_{wormhole}}{R_{node}} \times (1-\cos\theta) \quad (15)$$

Therefore, the value of $P_{wormhole}$ is computed as follows:

$$P_{wormhole} = \frac{1-\cos\theta'}{2} = \frac{R_{wormhole}}{R_{node}} \times \frac{(1-\cos\theta)}{2} \quad (16)$$

According to (11), it can be rewritten as:

$$P_{wormhole} = \frac{R_{wormhole}}{R_{node}} \times P_{legitimate} \quad (17)$$

Thus, it is concluded that the longer range of the wormhole is detected much easier and faster.

B. Artificial Immune System (AIS) based Learning Technique

Further, the other system parameters such as node density level, detection time variation, system overhead, storage overhead and wormhole range on attacker's risk are also considered with the maximum end-to-end delay, path length and conditional probabilities to detect the wormhole attacks efficiently. The considered parameters are learned by using AIS based on the clonal selection theory for detecting wormhole attacks with increased detection rate, speed and reduced computational complexity. In order to detect wormhole attacks, an immune system should achieve attack detection process such that the self-modules and cells may be differentiated from antigens. By immunology evolution, feasible antibodies that match a specific antigen are generated. The combination intensity between antigen and antibody is measured based on the affinity computations to direct the suppression of antibody generations.

- ***Affinity Computation:*** The Euclidean distance function is used for computing the affinity value between antibody and antigen. For each antibody (node)(n), consider two antigens (parameters)(x, y) and the distance between these two antigens is computed as follows:

$$d = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad (18)$$

The value of affinity $(f_i)$is computed as:

$$f_i = \frac{1}{d} \quad (19)$$

- ***Cloning:*** The cloning process is performed independently and proportionally to their antigenic affinity. It defines a higher the antigenic affinity, a higher the number of clones it produces. Each antibody generates the number of clones during the cloning process as:

$$c = \left[0.1 - \frac{f_i}{\sum_{i=1}^{b} f_i}\right] \times w \quad (20)$$

In equation (20), b is the number of antibody to be cloned and w is the number of wormhole links to be predicted. The clonal expansion process is used to generate a huge population of antibody-generating cells that are specific to the antigen. This results in destroying the antigen and retains some of these cells in immunological memory. Thus, any following exposure to a similar antigen directs to rapid immune response.

- ***Mutation:*** Here, two types of mutation technique are used such as Gaussian mutation and Cauchy mutation. The affinity measures from both techniques are compared to select the best possible solution i.e., wormhole link is predicted. The mutation process is inversely proportional to the antigenic affinity that means a higher the affinity, a smaller the mutation rate.
- ***Regression Test:*** Further, the accuracy of predicted wormhole links W after the testing process is determined by using the regression test that computes correlation coefficient to measure how fit the predicted values from a forecast model with the past actual values.The correlation coefficient $(\mathcal{R})$ as follows:

$$\mathcal{R} = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{[n\sum x_i^2 - (x_i)^2] \times [n\sum y_i^2 - (y_i)^2]}} \quad (21)$$

If the correlation coefficient is very low, then it is concluded that there is no relationship between the predicted values and the actual values. A perfect fit can give $\mathcal{R} = 1$, and so it is concluded that a higher correlation coefficient provides a better predicted value.

The algorithm steps of AIS using the clonal selection theory for wormhole attack detection are as follows:

Input: node density level, detection time variation, system overhead, storage overhead and wormhole range on attacker's risk, maximum end-to-end delay, path length and conditional probabilities

Output: Wormhole Link/Attack

Step 1: Initialize a population $(P)$of antibodies Ab randomly and split as two subsets as Ab_m (memory population) and Ab_p (pool population).

Step 2: Generate a set of antigenic patters Ag.

Step 3: Choose an antigen $Ag_i$from Ag.

Step 4: $for(each\ member\ of\ Ab)$

{

Compute Euclidean distance between two antigens;

Compute affinity value f_i to the antigenAg_i;

}

Step 5: Choose the top-k highest affinity antibodies and generate c clones for each Ab in proportion to their affinity, locating the clones in a new populationP_{new}.

Step 6: Mutate P_{new} to a degree inversely proportional to their affinity for generating a mature population P_{mnew}.

Step 7: Re-compute the affinity value to each member ofP_{mnew}.

Step 8: Choose the highest score as candidate memory cell. If its affinity is higher than the current memory cellAb_{mnew}, then the candidate becomes the new memory cell.

Step 9: Eliminate those antibodies with low affinity in Ab_p and replace them with new randomly generated members.

Step 10: Repeat Steps 3-9 until all antigens have been presented.

Thus, the training process is completed and the testing process is carried out to predict the wormhole links through the network. After that, the accuracy of wormhole attack detection is determined by using the regression test. The testing process is repeated until a higher value of correlation coefficient is obtained.

IV. RESULTS AND DISCUSSION

In this section, the performance of the proposed AIS-ISWAD technique is evaluated and compared with the existing ISWAD and SWAD techniques by using Network Simulator version 2.35 (NS2.35). This comparison is made in terms of different network metrics such as throughput, end-to-end delay, jitter, packet delivery ratio, packet loss ratio and detection rate. 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

A. Throughput

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

$$Throughput = \frac{Amount\ of\ packets\ correctly\ received\ by\ a\ destination}{Time\ taken} \quad (22)$$

Table 2 shows the comparison of proposed and existing techniques in terms of throughput.

Table 2: Comparison of Throughput

Techniques	Throughput (Kbps)
SWAD	7850
ISWAD	8350
AIS-ISWAD	8821

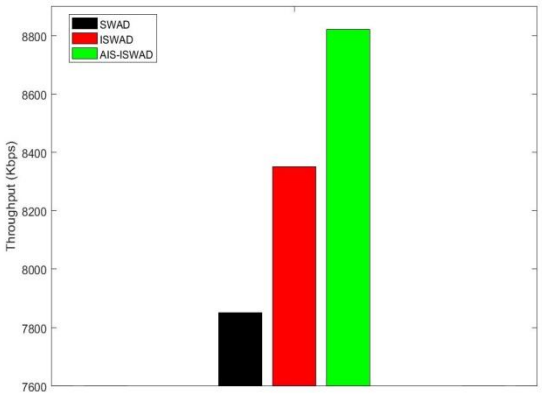

Fig.2: Comparison of Throughput

Fig. 2 shows that the comparison of AIS-ISWAD with ISWAD and SWAD techniques in terms of throughput taken in kbps. It is analyzed that the throughput of AIS-ISWAD technique is 5.64% higher than ISWAD technique and 12.37% higher than SWAD technique. From the analysis, it is observed that the throughput of the AIS-ISWAD technique increases than the other techniques.

B. End-to-end Delay

It refers the time taken to transmit the packets from source to destination and computed as:

$$Delay = \frac{Total\ time\ for\ packets\ received\ by\ the\ destination}{Total\ Number\ of\ packets\ received\ by\ the\ destination} \quad (23)$$

Table 3 shows the comparison of end-to-end delay for proposed and existing techniques.

Table 3: Comparison of End-to-end Delay

Techniques	End-to-end Delay (sec)
SWAD	3.6
ISWAD	2.5
AIS-ISWAD	1.9

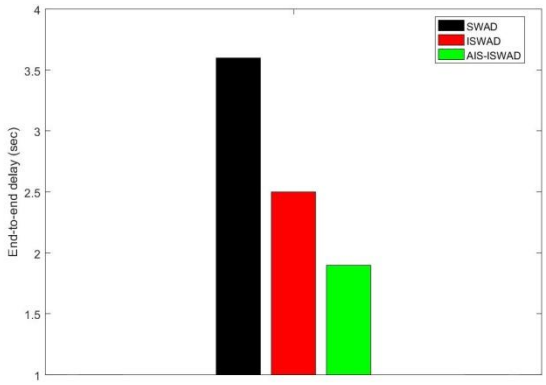

Fig.3: Comparison of End-to-end Delay

Fig. 3 shows that the comparison of AIS-ISWAD with ISWAD and SWAD in terms of end-to-end delay taken in seconds. It is analyzed that the end-to-end delay of AIS-ISWAD technique is 24% less than ISWAD technique and 47.22% less than SWAD technique. From the analysis, it is observed that the end-to-end delay of the proposed AIS-ISWAD technique decreases than the other techniques.

Table 4 shows the comparison of end-to-end delay for proposed and existing techniques according to the varying wormhole link length.

Table 4: Comparison of End-to-end Delay

Wormhole Length	SWAD	ISWAD	AIS-ISWAD
	End-to-end Delay (sec)		
1	0.145	0.139	0.131
2	0.154	0.148	0.139
3	0.165	0.160	0.146
4	0.170	0.166	0.155
5	0.18	0.176	0.162
6	0.184	0.180	0.170
7	0.189	0.184	0.178
8	0.194	0.190	0.185

Fig. 4 shows that the comparison of AIS-ISWAD with ISWAD and SWAD in terms of end-to-end delay in seconds according to the wormhole link length. It is analyzed that the end-to-end delay of AIS-ISWAD is 2.63% less than ISWAD and 4.64% decreased than SWAD technique when wormhole link length is considered as 8. From the analysis, it is observed that the end-to-end delay of the proposed AIS-ISWAD technique decreases in according to the varying wormhole link length than the existing techniques.

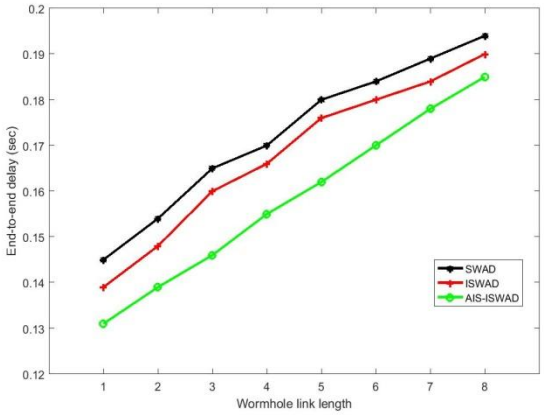

Fig.4: Comparison of End-to-end Delay

C. Jitter

It is defined as the variation in the delay of received packets.

Table 5 shows the comparison of proposed and existing techniques in terms of jitter.

Table 5: Comparison of Jitter

Techniques	Jitter (sec)
SWAD	25
ISWAD	19
AIS-ISWAD	13

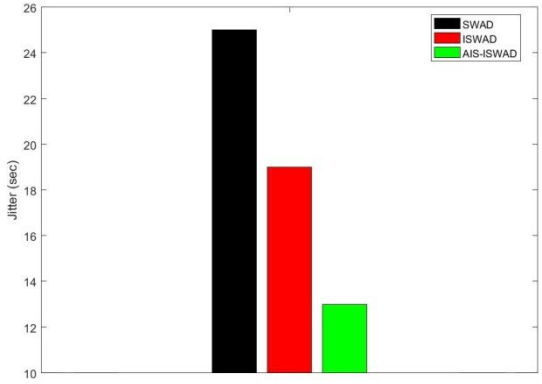

Fig.5: Comparison of Jitter

Fig. 5 shows that the comparison of AIS-ISWAD with ISWAD and SWAD in terms of jitter taken in seconds. It is analyzed that the jitter of AIS-ISWAD is 31.58% less than ISWAD technique and 48% reduced than SWAD technique. From the analysis, it is observed that the jitter of the AIS-ISWAD technique decreases than the other existing techniques.

D. Packet Delivery Ratio (PDR)

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:

$$PDR = \frac{Total\ number\ of\ packets\ received\ by\ destination}{Total\ number\ of\ packets\ transmitted\ by\ source} \times 100 \quad (24)$$

Table 6 shows the comparison of proposed and existing techniques in terms of PDR.

Table 6: Comparison of PDR

Techniques	PDR (%)
SWAD	95
ISWAD	95.6
AIS-ISWAD	96.5

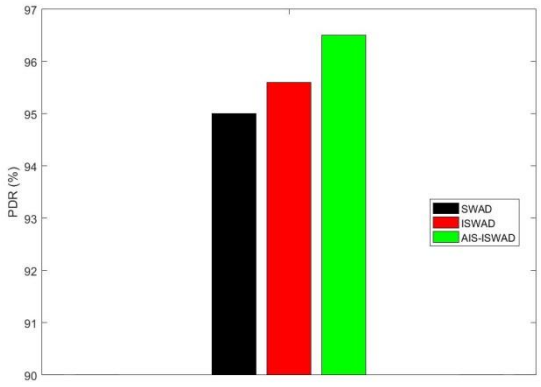

Fig.6: Comparison of PDR

Fig. 6 shows that the comparison of proposed and existing techniques such as AIS-ISWAD with ISWAD and SWAD in terms of PDR in %. It is analyzed that the packet delivery ratio of AIS-ISWAD technique is 0.94% higher than ISWAD technique and 1.58% higher than SWAD technique. From the analysis, it is observed that the packet delivery ratio of the AIS-ISWAD technique increases than the other techniques.

E. Packet Loss Ratio (PLR)

It defines the percentage of number of packets lost during transmission to the total number of packets sent from the source. It is calculated as:

$$PLR = \frac{Number\ of\ packets\ lost}{Total\ number\ of\ packets\ transmitted\ by\ source} \times 100 \quad (25)$$

Table 7 shows the comparison of proposed and existing techniques in terms of PLR.

Table 7: Comparison of PLR

Techniques	PLR (%)
SWAD	25.3
ISWAD	16
AIS-ISWAD	12.9

Fig. 7 shows that the comparison of AIS-ISWAD with existing ISWAD and SWAD in terms of PLR in %. It is analyzed that the packet loss ratio of AIS-ISWAD is 19.375% less than ISWAD technique and 48.4% reduced than SWAD technique. From the analysis, it is observed that the packet loss ratio of the AIS-ISWAD technique decreases than the other existing techniques.

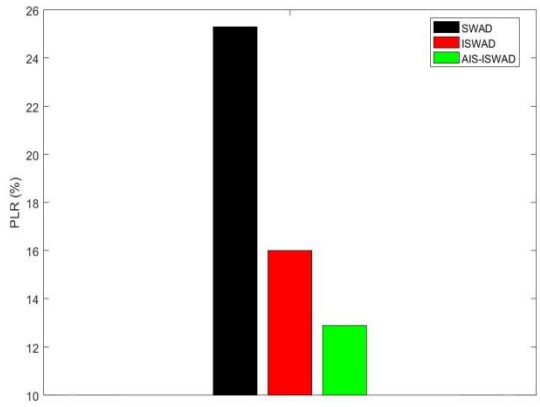

Fig.7: Comparison of PLR

F. Detection Rate

It defines the fraction of number of detected wormhole links to the total number of authentic wormhole links. Also, it is defined as the probability that all wormhole links are successfully detected. It is computed as:

$$Detection\ Rate = \frac{True\ Positive}{True\ Positive + False\ Negative} \times 100 \quad (26)$$

Table 8 shows the comparison of proposed and existing techniques in terms of detection rate.

Table 8: Comparison of Detection Rate

Techniques	Detection Rate (%)
SWAD	85
ISWAD	88.5
AIS-ISWAD	93

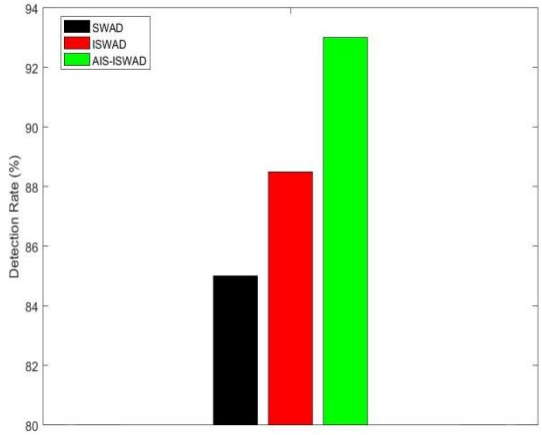

Fig.8: Comparison of Detection Rate

Fig. 8 shows that the comparison of AIS-ISWAD and existing ISWAD, SWAD in terms of detection rate in %. It is analyzed that the detection rate of AIS-ISWAD is 5.08% higher than ISWAD technique and 9.41% increased than SWAD technique. From the analysis, it is observed that the detection rate of the AIS-ISWAD technique increases than the other existing techniques.

V. CONCLUSION

In this article, an artificial immune system based learning technique is proposed to detect the wormhole links through the network. Based on this proposed AIS-ISWAD technique, the nodes in the network can be recognized that whether those are legitimate or illegitimate nodes. Hence, the packet loss and end-to-end delay due to transmitting the packets via illegitimate nodes i.e., attacked nodes is effectively avoided. As well, detection speed and accuracy are significantly increased. As a result, this technique can be very useful in real-time applications to prevent various attacks through the networks.

REFERENCES

1. M. Kumar and R. Mishra, "An overview of MANET: history, challenges and applications", Indian J. Comput. Sci. Eng., vol. 3, no. 1, pp. 121-125, 2012.
2. P. N. Reddy, CH. Vishnuvardhan and V. Ramesh, "Routing attacks in mobile adhoc networks", Int. J. Comput. Sci. Mob. Comput., vol. 2, no. 5, pp. 360-367, 2013.
3. S. Nivedha and S. S. Narayanan, "Detection and prevention of wormhole attack in MANET using new fresh algorithm", Int. J. Adv. Res. Comput. Eng. Technol., vol. 4, no. 5, pp. 2321-2326, 2015.
4. B. Awad and T. Barhoom, "BT-WAP: wormhole attack prevention model in MANET based on hop-count", Netw., vol. 4, no. 7, pp. 600-606, 2015.
5. P. Kaur, D. Kaur and R. Mahajan, "Wormhole attack detection technique in mobile ad hoc networks", Wirel. Personal Commun., vol. 97, no. 2, pp. 2939-2950, 2017.
6. M. Selladevi, T. Lathamaheswari and S. Duraisamy, "Improved secure aware wormhole attack detection in mobile ad-hoc networks", Int. J. Eng. Technol., vol. 7, no. 4, pp. 3472-3477, 2018.
7. M. Azer, S. El-Kassas and M. El-Soudani, "A full image of the wormhole attacks-towards introducing complex wormhole attacks in wireless ad hoc networks", Int. J. Comput. Sci. Inf. Secur., vol. 1, no. 1, pp.41-52, 2009.
8. F. Shi, D. Jin, W. Liu and J. Song, "Time-based detection and location of wormhole attacks in wireless ad hoc networks", in IEEE 10th Int. Conf. Trust, Secur. Priv. Comput. Commun., pp. 1721-1726, 2011.
9. S. Gupta, S. Kar and S. Dharmaraja," WHOP: Wormhole attack detection protocol using hound packet", in IEEE Int. Conf. Innov. Inf. Technol., pp. 226-231, 2011.
10. P. Nayak, A. Sahay and Y. Pandey, "Detection and prevention of wormhole attacks in Manets using detection packet", Int. J. Sci. Eng. Res., vol. 4, no. 6, pp. 1216-1222, 2013.
11. U. K. Chaurasia and V. Singh, "MAODV: Modified wormhole detection AODV protocol", in 6th Int. Conf. Contemp. Comput., pp. 239-243, 2013.
12. T. Giannetsos and T. Dimitriou, "LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks", J. Comput. Syst. Sci., vol. 80, no. 3, pp. 618-643, 2014.
13. R. Singh, J. Singh and R. Singh, "WRHT: a hybrid technique for detection of wormhole attack in wireless sensor networks", Mob. Inf. Syst., 2016.
14. S. Khobragade and P. Padiya, "Detection and prevention of wormhole attack based on delay per hop technique for wireless mobile ad-hoc network", in Int. Conf. Signal Process. Commun. Power Embed. Syst., pp. 1332-1339, 2016.
15. S. Bagade and V. Raisinghani, "JITWORM: Jitter monitoring based wormhole attack detection in MANET", in Int. Conf. Inf. Syst. Secur., Springer, Cham, pp. 444-458, 2016.
16. J. Kurmi, R. S. Verma and S. Soni, "An efficient and reliable methodology for wormhole attack detection in wireless sensor network", Adv. Comput. Sci. Technol., vol. 10, no. 5, pp. 1129-1138, 2017.
17. M. N. A. Shaon and K. Ferens, "A computationally intelligent approach to the detection of wormhole attacks in wireless sensor networks", Adv. Sci. Technol. Eng. Syst. J., vol. 2, no. 3, pp. 302-320, 2017.

AUTHORS PROFILE

M. Selladevi has received her Bachelor of Computer science from Bharathiar University in 2010, Master of Computer Science from Bharathiar University in 2012, M.Phil from Bharathiar University in 2014 and pursuing Ph.D. in Computer Science as Research Scholar in the Department of Computer Science in chikkanna Govt Arts College, Tamilnadu, India. Area of interests is Wireless Network and Mobile Computing.

Dr. T. Latha Maheswari has received her Bachelor of Science in Computer Technology from Bharathiar University in 1995, Master of Computer Applications from Bharathiar University in 1998 , M.Phil from Mother Teresa University in 2002 , M.E (Computer Science and Engineering) from Anna University in 2006 and Ph.D (Computer Science and Engineering) from Anna University in 2018. She is currently working as Associate Professor in Sri Krishna College of Engineering and Technology. Her research interests cover the Object Oriented Systems, Sensor networks, Neural Networks and Web Queering with over 10 technical publications. She has 19 years of teaching experience.

Dr. S. Duraisamy has received his Bachelor of Science in Computer Science from Bharathiar University in 1994, Master of Computer Applications from Bharathiar University in 1997, M.Phil from MS University in 2002 and Ph.D (Computer Science) from Alagappa University in 2008. He is currently working as Assistant Professor in Chikkanna Government Arts College. His research interests cover the Object Oriented Systems, Sensor networks, Neural Networks and Web Queering with over 60 technical publications. He has 22 years of teaching experience.