A Hybridized Immune System for Avoidance of Wormhole Attacks in Manet

M. Selladevi, T. Lathamaheswari, S. Duraisamy

Abstract*: *In Mobile Ad-hoc Networks (MANETs), the most challenging task is detecting and mitigating wormhole links during data transmission between the source and destination nodes. Since it requires special hardware, synchronized clocks, mobile nodes equipped with GPS, etc. To overcome these challenges, Artificial Immune System-based Improved Secure-aware Wormhole Attack Detection (AIS-ISWAD) technique has been proposed that considers maximum end-to-end delay, path length and system parameters for detecting wormhole attacks. To simplify the detection process, AIS has been used as a learning approach that learns those parameters to detect the wormhole links and select an alternative route for transmitting the data packets. However, an uncertainty problem is addressed in AIS during computation of affinity value between antibody and antigen. Also, route selection is still not satisfied since data transmission requires a high-performance stable path from source to destination nodes. Therefore, the main goal of this article is handling the uncertainty problem during affinity computation and selecting the high-performance stable paths to transmit the data. In this paper, a Fuzzy Logic and AIS-ISWAD (FLAIS-ISWAD) technique is proposed to improve the wormhole attack detection and mitigation. In this technique, all computed parameters are given to the FL system to handle the uncertainty problem and construct the high-performance stable paths among all available paths in the network. Also, AIS is applied as a learning method to identify and isolate the wormhole links/nodes in MANETs with the highest network performance. Finally, the performance of the FLAIS-ISWAD technique is evaluated and compared through simulation results in terms of different performance metrics.

Index Terms*: *MANET, Wormhole links, Routing protocol, AIS-ISWAD, Fuzzy logic

I. INTRODUCTION

MANET is a kind of wireless network which contains many self-configuring mobile nodes. These mobile nodes are travelling independently in any direction within their transmission range; but, this independent mobility can affect the network topology. Due to these frequent changes in the network topology, scalability and network performance are degraded [1]. Also, MANETs are vulnerable to several types of attacks such as wormhole, blackhole, grayhole, etc. Among those attacks, wormhole attacks are not easily detected since an invader does not require any break to launch wormhole attacks in the network.

Specifically, wormhole attacks are a severe attack on MANET routing where two invaders linked by a high-speed off-channel link called the wormhole link. The wormhole link may be established by using a network cable and any form of wired connection technology or a long-range wireless communication in a different band. The end-point of this link i.e., wormhole node is equipped with radio transceivers compatible with the ad-hoc or sensor network to be attacked. Once the wormhole link is established, the opponent traces the wireless data they overhear, transmits it to each other and replays the packets via the wormhole link at the other end of the network. Replaying legitimate network messages at improper locations, wormhole attackers may make far apart nodes believe they are immediate neighbors and force all transmissions between artificial nodes [2]. Generally, ad-hoc routing protocols are divided into two types, namely proactive and reactive protocols. Proactive routing protocols rely on the periodic transmission of routing updates whereas reactive routing protocols search paths only when it is needed. A wormhole attack is evenly hazardous for both proactive and reactive protocols. For this reason, wormhole attack/link detection in the network is very essential. In the past decades, few researchers have practiced on detecting and preventing the wormhole attacks in the networks.

Recently, Kaur et al. [3] proposed a novel SWAD technique based on the maximum end-to-end delay between two nodes within the transmission range. It does not require the mobile nodes to be equipped with GPS, clock synchronization or any other type of special hardware. On the other hand, the length of paths passing through the wormhole attackers is not taken into account during detection. When the attackers are located in the chosen path, the path length may be reduced considerably. Therefore, Selladevi et al. [4-5] proposed an ISWAD technique by considering both path length and the maximum end-to-end delay for wormhole attacks/links in MANETs. Conversely, more parameters are required to increase detection accuracy efficiently. As a result, AIS-ISWAD technique is proposed in which system parameters are also taken into account to detect the wormhole links. These various parameters are effectively learned by the AIS for increasing the detection performance extensively.

Also, a scalable and distributed scheme is introduced by using the sequential probability ratio test model to isolate single-point failures and high mobility of nodes. Nonetheless, a high-performance stable path from all available paths does not well differentiate.

Revised Manuscript Received on October 15, 2019.

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.

Also, an uncertainty arises during computation of affinity value between antibody and antigen.

Hence, this article focuses on handling this uncertainty problem and finding a high-performance stable path among all available paths. An FLAIS-ISWAD technique is proposed as an improvement of AIS-ISWAD to detect the wormhole links/attacks in Ad-hoc On-demand Distance Vector (AODV) routing protocols. Initially, maximum end-to-end delay, path length and system parameters are computed between the source and destination nodes. Then, these parameters are given to the fuzzy logic system to differentiate the high-performance stable paths among available paths and handle an uncertainty problem in affinity computation. Additionally, AIS is applied as a learning process to detect and the wormhole attacks/links without affecting the overall network performance. Thus, the wormhole nodes in MANETs are efficiently detected and prevented with the highest detection accuracy. Also, an uncertainty problem during affinity computation between antibody and antigen is handled.

The remaining article is structured as follows: Section II discusses the related works on the detection and prevention of wormhole attacks in MANET. Section III explains the methodology of the proposed FLAIS-ISWAD technique. Section IV shows the simulation results of FLAIS-ISWAD technique compared with the existing techniques. Section V gives the conclusion for the entire work.

II. LITERATURE SURVEY

Shamaei & Movaghar [6] proposed a two-phase wormhole attack detection scheme in MANETs. The first phase was used to check whether a wormhole tunnel exists on the chosen route or not. If there was such a tunnel, the second phase was applied for confirming the existence of the wormhole attack and locating a malicious node. However, the detection time and false positive rate of this method were high. Imran et al. [7] analyzed different wormhole detection techniques and identified a few common limitations of those techniques which may affect the performance of MANETs in different ways. Also, the features of MANETs were identified based on which wormhole attacks can be detected. However, they identified that the techniques based on Route Request (RREQ) or hop count were not effective to detect wormhole attacks.

Amish & Vaghela [8] surveyed different techniques dealing with wormhole attack and proposed a method for detecting and preventing wormhole attacks. In this method, Ad-hoc On-demand Multipath Distance Vector (AOMDV) routing protocol was incorporated based on Round Trip Time (RTT) mechanism and other features of the wormhole attack. However, the average end-to-end delay was high. Bagade & Raisinghani [9] proposed Jitter monitoring-based Wormhole (JITWORM) attack detection in MANET. In this method, the wormhole attack was detected during the route discovery phase and data transmission phase. The wormholes were detected by employing a mechanism of analyzing the jitter applied to packets by the nodes. If the percentage of packets to which jitter was not applied was greater than a set threshold, then a wormhole was considered to be present. Once wormhole was detected, it may be prevented from the network. However, it needs to detect wormholes during RREP based on link analysis by the neighboring nodes.

Shaon & Ferens [10] proposed a computationally intelligent approach to detect the wormhole attacks. In this approach, an Artificial Neural Network (ANN) was proposed for detecting the possible locations of wormhole nodes in both equally and non-equally distributed sensor networks. Nonetheless, an exact location of wormhole nodes was not efficiently detected.

Kurmi et al. [11] proposed an efficient and reliable wormhole attack method for detecting wormhole attacks. Also, a localization-based scheme was proposed for minimizing the detection cost of wormhole attacks based on the key observation that a large number of network traffic was concerned by the wormholes. Nevertheless, this method has energy consumption and simulation time.

Rmayti et al. [12] proposed graph-based wormhole attack detection in MANETs. The main goal of this method was to use reactive routing protocols for detecting wormhole attacks. This method was based on the routing information contained in the exchanged messages and the routing tables of nodes. However, it requires the isolation of wormholes based on the time travel of RREQ messages between every two successive nodes in suspect routes.

III. PROPOSED METHODOLOGY

In this section, the proposed FLAIS-ISWAD technique is briefly explained. At first, the network is built by using the N number of mobile nodes and M number of attackers. Each node must be homogeneous, symmetric and dynamic. Also, each node has n neighboring nodes for constructing many disjoint routes. The data transmission is established between the source and destination nodes at a specific communication range. Let two nodes connect each other through an out-of-band channel which is known as wormhole link. This wormhole link can be detected and prevented by the proposed FLAIS-ISWAD technique by taking into consideration of maximum end-to-end delay, path length and system parameters such as node density, system/network overhead, network capacity (storage) and detection time deviation measure. The flow diagram of FLAIS-ISWAD is shown in Fig. 1.

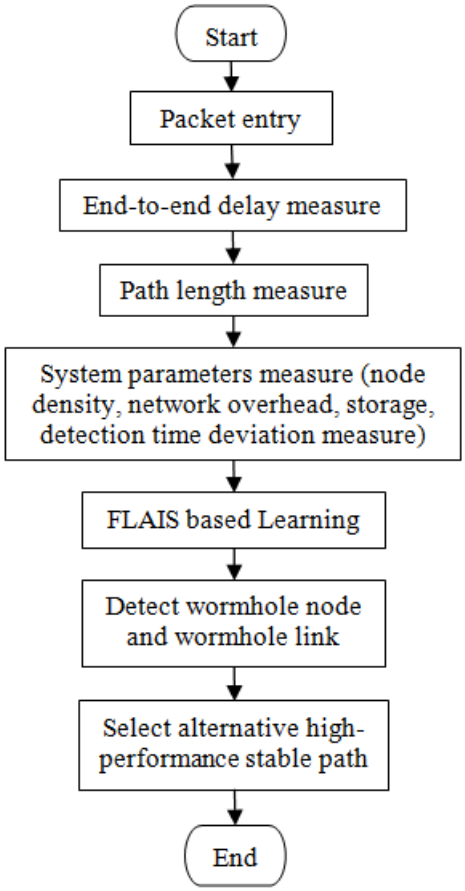

Fig.1: Flow Diagram of FLAIS-ISWAD Technique

A. Fuzzy Logic for High-Performance Stable Path Selection

Initially, the FL system is applied to solve the uncertainty of affinity value between antibody and antigen in AIS for selecting the high-performance stable paths among all possible paths between the source and destination nodes. To achieve this, different parameters i.e., maximum end-to-end delay, path length, residual energy, hop count and system parameters such as node density, system/network overhead, network capacity (storage) and detection time deviation measure are used. The major processes of FL system are shown in Fig. 2. They are fuzzification, fuzzy inference and defuzzification.

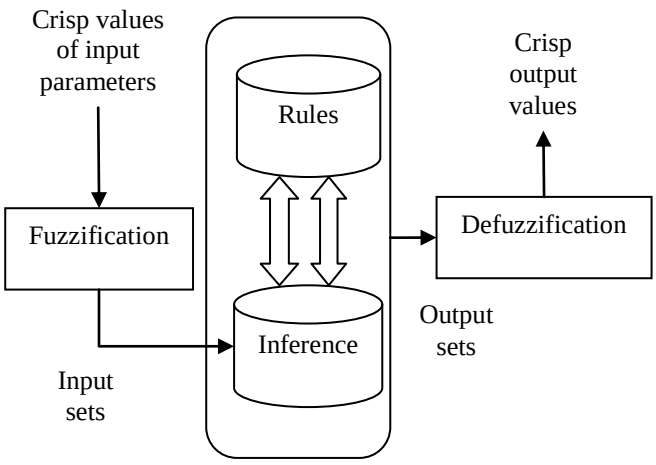

Fig.2: Major Processes in FL System

Phase 1: Fuzzification

In this phase, the considered input parameters are fuzzified in terms of 9 linguistic terms such as Low-Low (LL), Low-Medium (LM), Low-High (LH), Medium-Low (ML), Medium-Medium (MM), Medium-High (MH), High-Low (HL), High-Medium (HM) and High-High (HH). The linguistic set always the interval between 0 and 1. The output of this FL system is a set of fuzzy variables known as fuzzy path priority. These variables provide the fitness of any path in terms of performance. Fig. 3 & 4 show the fuzzy membership function for input variables and the output variable.

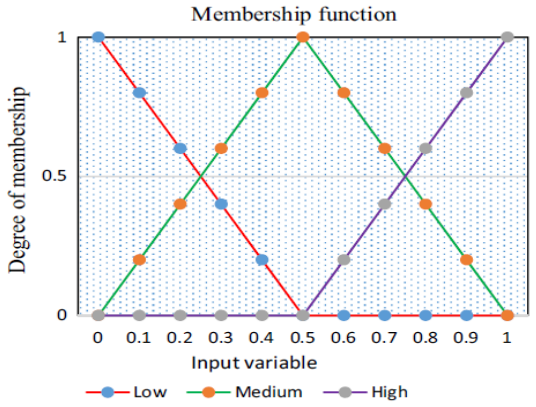

Fig.3: Sample Fuzzy Membership Function for Input Variable

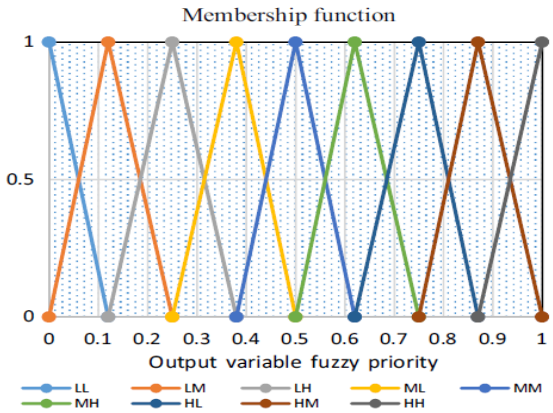

Fig.4: Fuzzy Membership Function for Output Variable

Phase 2: Inference Engine and Knowledge Base

Knowledge is a set of rules developed by an expert system. These rules link inputs and outputs. The fuzzy rules are in the form of IF-THEM configuration. The inputs are combined by using the AND-OR operators. The sample fuzzy rules are given in Table 1.

Table 1: Sample Fuzzy Rules for Fuzzification

End-to-end delay	Path length	Hop count	Node density	System overhead	Detection time deviation	Residual energy	Network capacity	Fuzzy path priority
L	L	L	L	L	L	H	H	HH
L	L	L	L	L	L	M	M	HM
L	M	L	L	L	L	L	L	HL
M	L	M	M	L	M	H	H	MH
M	M	M	M	M	M	M	M	MM
L	L	M	M	M	L	L	L	ML
M	M	H	H	M	L	H	H	LH
H	H	H	H	H	H	M	M	LM
H	H	H	H	H	H	L	L	LL

Phase 3: Defuzzification

In this proposed technique, the maximum defuzzifiers are used i.e., the paths with the priority levels of HH, HM and HL are chosen as the high-performance stable path among all available paths.

B. AIS-based Wormhole Attack Detection

In the AODV routing protocol, the primary RREP (Route Reply) is received by the source node, the data packets will be sent to the destination node. But, in this proposed technique, the data packets are not transmitted directly towards the destination node based on the primary RREP reception. Relatively, the source node considers all received RREPs and then chooses the most secure path by the AIS [5] which detects the wormhole link in the network. This approach is performed based on the human immune system, where antibodies are trained for detecting and mitigating the malicious (wormhole) antigens. Therefore, this approach can develop and update a set of conditions i.e., fuzzy rules that could detect the paths passed through the wormhole attackers and mitigate from choosing them.

Among all high-performance stable paths selected by FL, the immune paths are chosen by detecting the wormhole links/attacks by this AIS approach. Table 2 represents the mapping between the human body and MANET.

Table 2: Mapping between AIS and MANETs

Human Body	MANETs
Self-cells	Well-behaving nodes
Non-self-cells	Wormhole nodes
Antigen	Conditions set for limiting wormhole attacks i.e., available parameters and conditional probabilities
Antibody	All paths between source and destination node
Chemical binding of antibodies to antigens	Matching function between detectors and antibodies
Colonization	Regeneration on antibodies with the most antigens adaptation
Affinity	Distance between two nodes/hop count
Mutation	Comparison between hop count and selection of that path which has the primary RREP

The AIS consists of a detection part that is based on a continuous training process. This training of the detectors has different elements such as an antibody, antigen (available parameters and conditional probabilities computed by Sequential Probability Ratio Test (SPRT)) and reject, match with self and non-self, completion of detector set, safety memory and hypermutation. The processes in this approach are affinity computation, cloning and mutation [5].

Once the training process is finished, the testing process is carried out to detect the wormhole links and mitigate these links/attacks by selecting the most secured high-performance stable path for data transmission. The testing process is continued until a higher value of correlation coefficient is reached. Then, the regression test is used for evaluating the detection ratio of the proposed technique.

IV. SIMULATION RESULTS

In this section, the performance efficiency of the proposed FLAIS-ISWAD technique is analyzed and compared with the existing AIS-ISWAD and ISWAD techniques in terms of throughput, end-to-end delay, jitter, PDR, PLR and detection rate. This analysis is achieved by simulating these techniques by using Network Simulator (NS2.35). The simulation parameters are listed in Table 3.

Table 3: 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 is referred to as the number of data packets successfully delivered to the destination node in a given time.

$$Thr = \frac{No.of\ data\ packets\ successfully\ delivered\ to\ the\ destination\ node}{Time\ period}$$

Table 4 shows the comparison of proposed and existing techniques in terms of throughput.

Table 4: Comparison of Throughput

Techniques	Throughput (Kbps)
ISWAD	8350
AIS-ISWAD	8821
FLAIS-ISWAD	9364

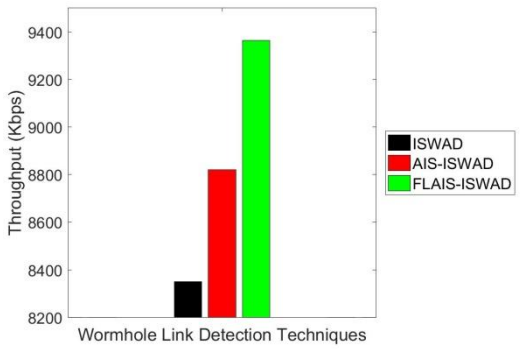

Fig.5: Comparison of Throughput

In Fig. 5, the comparison of FLAIS-ISWAD with AIS-ISWAD and ISWAD techniques are shown in terms of throughput (in kbps). The throughput of FLAIS-ISWAD technique is 6.16% higher than AIS-ISWAD and 12.14% higher than ISWAD technique. From this analysis, it is observed that the proposed FLAIS-ISWAD technique has better throughput than the AIS-ISWAD and ISWAD techniques.

B. End-to-end Delay

It is referred to as the time taken for transmitting the data packets between the source node and destination node.

$$E2E\_D = \frac{Total\ time\ for\ data\ packets\ received\ by\ the\ destination}{Total\ No.of\ data\ packets\ received\ by\ the\ destination}$$

Table 5 shows the comparison of end-to-end delay for proposed and existing techniques.

Table 5: Comparison of End-to-end Delay

Techniques	End-to-end Delay (sec)
ISWAD	2.5
AIS-ISWAD	1.9
FLAIS-ISWAD	1.3

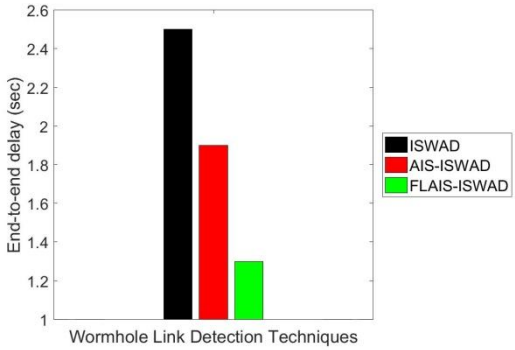

Fig.6: Comparison of End-to-end Delay

In Fig. 6, the comparison of FLAIS-ISWAD with AIS-ISWAD and ISWAD techniques are shown in terms of end-to-end delay (in seconds). The end-to-end delay of FLAIS-ISWAD technique is 31.58% reduced than AIS-ISWAD and 48% reduced than ISWAD technique. From this analysis, it is observed that the proposed FLAIS-ISWAD technique has minimized end-to-end delay than the AIS-ISWAD and ISWAD techniques.

Table 6 shows the comparison of end-to-end delay for proposed and existing techniques according to the varying wormhole link length.

Table 6: Comparison of End-to-end Delay

Wormhole Length	ISWAD	AIS-ISWAD	FLAIS-ISWAD
	End-to-end Delay (sec)		
1	0.139	0.131	0.123
2	0.148	0.139	0.130
3	0.160	0.146	0.137
4	0.166	0.155	0.143
5	0.176	0.162	0.150
6	0.180	0.170	0.157
7	0.184	0.178	0.164
8	0.190	0.185	0.172

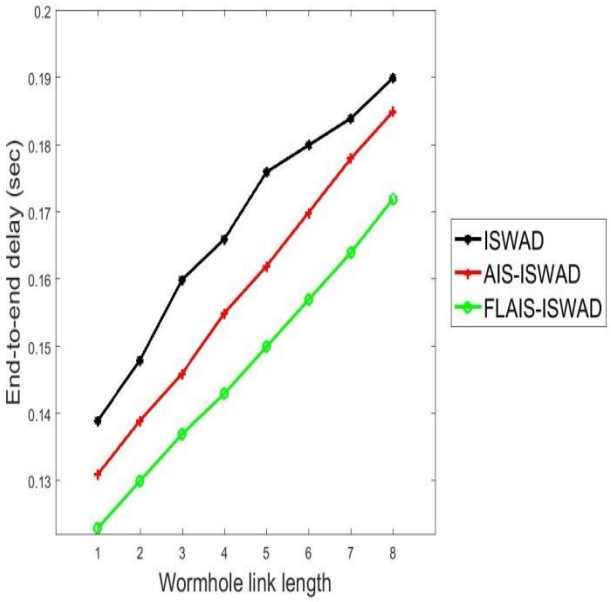

Fig.7: Comparison of End-to-end Delay

In Fig. 7, the comparison of FLAIS-ISWAD with AIS-ISWAD and ISWAD techniques are shown in terms of end-to-end delay (in seconds) for varying wormhole link length. When the wormhole link length is taken as 8, the end-to-end delay of FLAIS-ISWAD technique is 7.03% less than AIS-ISWAD and 9.47% less than ISWAD technique. From this analysis, it is observed that the proposed FLAIS-ISWAD technique has reduced end-to-end delay than the AIS-ISWAD and ISWAD techniques.

C. Jitter

It is referred to as the delay deviation of the received data packets.

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

Table 7: Comparison of Jitter

Techniques	Jitter (sec)
ISWAD	19
AIS-ISWAD	13
FLAIS-ISWAD	7

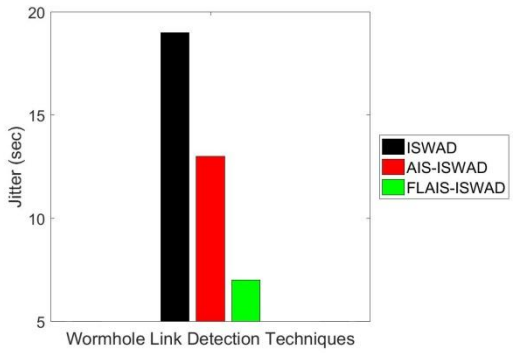

Fig.8: Comparison of Jitter

In Fig. 8, the comparison of FLAIS-ISWAD with AIS-ISWAD and ISWAD techniques are shown in terms of jitter (in seconds). The jitter of FLAIS-ISWAD technique is 46.15% reduced than AIS-ISWAD and 63.16% reduced than ISWAD technique. From this analysis, it is observed that the proposed FLAIS-ISWAD technique has less jitter than the AIS-ISWAD and ISWAD techniques.

D. Packet Delivery Ratio (PDR)

It is referred to as the fraction between the total amount of data packets delivered to the destination and total amount of data packets transmitted from the source node.

$$PDR = \frac{Total\ No.of\ data\ packets\ received\ by\ the\ destination\ \ node}{Total\ No.\ of\ data\ packets\ transmitted\ \ by\ the\ source\ node} \times 100\%$$

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

Table 8: Comparison of PDR

Techniques	PDR (%)
ISWAD	95.6
AIS-ISWAD	96.5
FLAIS-ISWAD	97.6

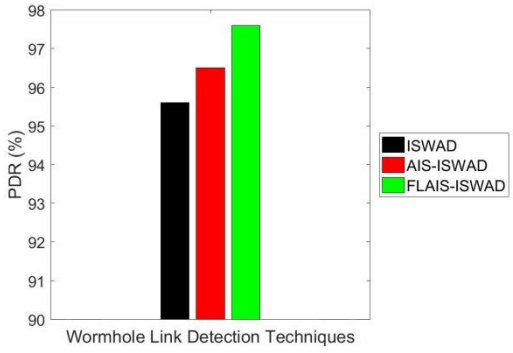

Fig.9: Comparison of PDR

In Fig. 9, the comparison of FLAIS-ISWAD with AIS-ISWAD and ISWAD techniques are shown in terms of PDR (in %). The PDR of FLAIS-ISWAD technique is 1.14% higher than AIS-ISWAD and 2.09% higher than ISWAD technique. From this analysis, it is observed that the proposed FLAIS-ISWAD technique has higher PDR than the AIS-ISWAD and ISWAD techniques.

E. Packet Loss Ratio (PLR)

It is referred to as the fraction between the total number of data packets missing in the data transmission and the total number of data packets transmitted from the source node.

$$PLR = \frac{No.of\ data\ packets\ \ lost}{Total\ No.of\ data\ packets\ \ transmitted\ \ by\ the\ source\ \ node} \times 100\%$$

Table 9 shows the comparison of proposed and existing techniques in terms of PLR.

Table 9: Comparison of PLR

Techniques	PLR (%)
ISWAD	16
AIS-ISWAD	12.9
FLAIS-ISWAD	8.1

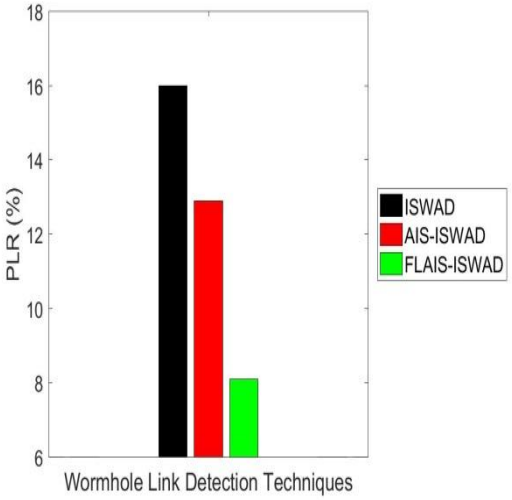

Fig.10: Comparison of PLR

In Fig. 10, the comparison of FLAIS-ISWAD with AIS-ISWAD and ISWAD techniques are shown in terms of PLR (in %). The PLR of FLAIS-ISWAD technique is 37.21% less than AIS-ISWAD and 49.38% less than ISWAD technique. From this analysis, it is observed that the proposed FLAIS-ISWAD technique has minimum PLR than the AIS-ISWAD and ISWAD techniques.

F. Detection Rate

It is referred to as the percentage between the total number of detected wormhole links/nodes/attacks and the actual number of wormhole links in the network. In other words, it is the prospect that all wormhole links are successfully detected.

$$Detection\ Rate = \frac{True\ \ Positive}{True\ \ Positive + False\ \ Negative} \times 100\%$$

Here, true positive is an outcome where FLAIS-ISWAD correctly detects the wormhole links/attacks/nodes as itself. Conversely, false negative is an outcome where FLAIS-ISWAD incorrectly detects the non-wormhole links as wormhole links.

Table 10 shows the comparison of proposed and existing techniques in terms of detection rate.

Table 10: Comparison of Detection Rate

Techniques	Detection Rate (%)
ISWAD	88.5
AIS-ISWAD	93
FLAIS-ISWAD	95.6

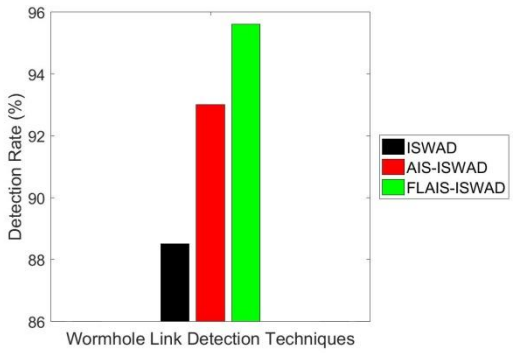

Fig.11: Comparison of Detection Rate

In Fig. 11, the comparison of FLAIS-ISWAD with AIS-ISWAD and ISWAD techniques are shown in terms of detection ratio (in %). The detection ratio of FLAIS-ISWAD technique is 2.8% higher than AIS-ISWAD and 8.02% higher than ISWAD technique. From this analysis, it is observed that the proposed FLAIS-ISWAD technique has higher detection ratio than the AIS-ISWAD and ISWAD techniques.

V. CONCLUSION

In this article, a FLAIS-ISWAD technique is proposed for wormhole attack detection and mitigation in MANETs. At first, the required parameters such as maximum end-to-end delay, path length, and different system parameters are computed. Then, these parameters are converted into fuzzy linguistic variables and given to the FL system to obtain the fuzzy path priority. Based on this fuzzy path priority, the high-performance stable paths among all available paths are selected in the network. Also, the uncertainty problem during affinity computation in AIS is handled by these fuzzy variables. Moreover, the AIS approach is applied to learn all these parameters for detecting wormhole links/attacks in the network. Once the wormhole links are detected, then an alternative high-performance stable path is chosen for data transmission. Finally, the simulation results proved that the proposed FLAIS-ISWAD technique has better performance than the existing wormhole attack detection techniques in terms of throughput, end-to-end delay, jitter, packet delivery ratio, packet loss ratio and detection ratio. This technique can be useful to detect the different attacks in the real-time applications with better accuracy.

REFERENCES

1. A. Gupta, P. Verma and R. S. Sambyal, “An overview of MANET: features, challenges and applications”, in Natl. Conf. Recent Adv. Comput. Sci. IT, Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 4, no. 1, pp. 122-126, 2018.
2. A. P. Rai, V. Srivastava and R. Bhatia, “Wormhole attack detection in mobile ad hoc networks”, Int. J. Eng. Innov. Technol., vol. 2, no. 2, pp. 384-389, 2012.
3. P. Kaur, D. Kaur and R. Mahajan, “Wormhole Attack Detection Technique in Mobile Ad Hoc Networks”, Wirel. Pers. Commun., vol. 97, no. 2, pp. 2939-2950, 2017.
4. 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.
5. M. Selladevi, T. Lathamaheswari and S. Duraisamy, “Artificial immune system based improved secure-aware wormhole attack detection in MANET”, Int. J. Recent Technol. Eng., vol. 8, no. 2, pp. 2834-2841, 2019.
6. S. Shamaei and A. Movaghar, “A Two-Phase Wormhole Attack Detection Scheme in MANETs”, ISeCure, vol. 6, no. 2, pp. 183-191, 2014.
7. M. Imran, F. A. Khan, T. Jamal and M. H. Durad, “Analysis of detection features for wormhole attacks in MANETs”, Procedia Comput. Sci., vol. 56, pp. 384-390, 2015.
8. P. Amish and V. B. Vaghela, “Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol”, Procedia computer science, vol. 79, pp. 700-707, 2016.
9. 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.
10. 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.
11. 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.
12. M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi and A. Mammeri, “Graph-based wormhole attack detection in mobile ad hoc networks (manets)”, in IEEE 4th Int. Conf. Mob. Secur. Serv., pp. 1-6, 2018.

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.