Exclusion of Wormhole and Blackhole Attacks in Manets using Fuzzy Lamport Timestamp Algorithm

P.S. Hiremath
Dept of Computer Science MCA),
KLE Technological University,
BVBCET, Hubballi-580031, India
hiremathps53@yahoo.com

Anuradha T.
Dept of Computer Science and Engg,
PDA College of Engg
Kalaburagi, India
anuradhat26@gmail.com

Prakash Pattan
Dept of Computer Science and Engg,
PDA College of Engg
Kalaburagi, India
prakashpattan@gmail.com

Abstract- Security for any network is a primary concern as it is necessary to safeguard the resources that are being shared. A mobile ad-hoc network (MANET) enables the mobile devices to form a temporary network without any centralized infrastructure. MANET is vulnerable to several attacks, e.g. wormhole and blackhole attacks. Since there is increase in use of wireless communication, minimizing the intruders in wireless networks has been a high priority task. These attacks affect directly the performance of network. Eliminating such attacks in MANET is a challenging task. In this paper, a novel method that excludes the packets of wormhole and blackhole attacks in a MANET using fuzzy Lamport timestamp algorithm (FLTA) is proposed. The proposed FLTA is used to identify the order of event and to make synchronization of time clock in network device. The Lamport timestamp algorithm incorporates a fuzzy inference system to improve the performance of network. The simulated results of the proposed algorithm are compared with that of LTAWB [13] and SMTWB [12] for wormhole and blackhole attacks. It is observed that the proposed FLTA shows better performance as compared to LTAWB and SMTWB protocols in terms of throughput, end-to-end delay and packet delivery ratio.

Keywords*: MANET, FLTA, LTAWB, Wormhole, Blackhole, Fuzzy inference system, Lamport timestamp, AODV routing protocol multipath routing, security attacks.*

*****

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a wireless network in which, a group of mobile devices (nodes) form a provisional network without the aid of any established centralized coordinator. Each node acts as a host and a router at the same time. Each node participating in a MANET commits itself to forward data packets from a neighboring node to another node until a final destination is reached. The survival of a MANET relies on the cooperation between its participating members (or nodes) in the network. The nodes are free to move randomly and thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand alone fashion, or may be connected to the larger internet. All the nodes in the network participate in the routing and the performance solely depends on the cooperation between the participating nodes. The main objective of MANET routing protocols is to improve performance of network by minimizing delay, maximizing throughput and network lifetime. Some of the key characteristics of MANETs that affect the performance of the network are: dynamic network topology, bandwidth links and energy constrained operations. Another important factor that play a vital role in MANET performance is routing. The four basic routing functionalities for mobile ad-hoc networks are: path generation, path selection, data forwarding and path maintenance. Basically, MANETs are weak in preserving their own resources from attacks, and hence, are vulnerable to many security attacks. There are four types of security attacks, namely, Active, Passive, Internal and External attacks.

In active attacks, attackers interrupt the regular functioning of the network by dropping or modifying the exchanged packets. Such attacks may occur in physical layer, data link layer, network layer, transport layer and application layer. In the network layer, attacks like, Wormhole, Blackhole, Byzantine flooding, Resource consumption and Location disclosure are the examples of active attacks.

In passive attacks, attackers snoops the private information of packets without modifying it. The attacks like, traffic analysis, monitoring, eavesdropping, are categorized as passive attacks.

In internal attacks, attackers are members of the same network and nodes are of compromised type.

In external attacks, attackers are outside the network and carryout through the nodes that are not considered in the network. In this paper, the security attacks, namely, wormhole and blackhole attacks, which belong to the active attacks category, are investigated.

A. Wormhole attack

One of the most severe attack in MANETs is the wormhole attack. In this attack, an attacker records packets at one location in the network and tunnels them to another location. This tunnel between two colluding nodes is referred as wormhole attack (Fig.1). Routing of packets is disrupted when routing control messages are tunneled. Generally, AODV routing protocol is used to filter the wormhole packets. This routing protocol is responsible for finding the shortest path with less traffic, but it is more challenging task to maintain the route for very long time. Now the wormhole node becomes greedy and utilizes this shortest path, by creating a tunnel over the network and present an false impression of shortest path via wormhole nodes. The Fig.1 shows that, 'S' is source node and 'D' is the destination node, a wormhole tunnel is formed from W1 to W2. The packets flow through wormhole tunnel, from one end (W1) to other end (W2), without reaching the destination.

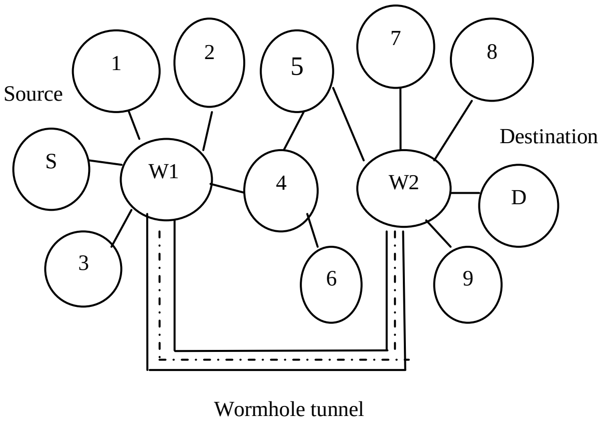

Figure 1. Wormhole attack in network

B. *Blackhole attack*

Among various attacks in MANETs, blackhole is considered as yet another severe attack. A blackhole is said to be a wicked node that incorrectly replies to route requests without having an active route to the destination. It exploits the routing protocol to advertise itself as having a shortest route to destination. It is depicted in the Fig.2 that the node B1 is a source node and B5 is a destination node. The node BH is blackhole, node B2 and node BH are the neighboring nodes of source node B1. When source node B1 send a RREQ (Routé request) packet to its neighboring nodes BH node replies immediately with RREP (Route reply) packet to source node B1. In case, the response from the node BH reaches to node B1 at the earliest, then source node ignores all other RREPs and starts to send data packets to BH which absorbs all data packets from node B1 and BH node becomes a black hole.

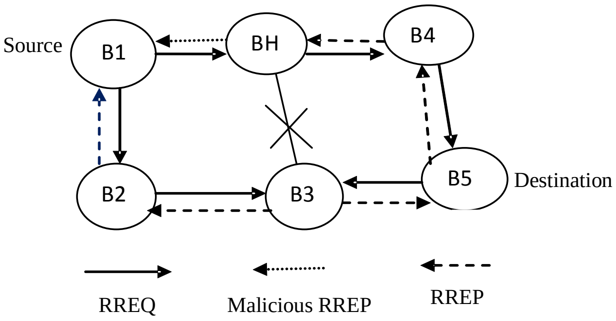

Figure 2. Blackhole attack in network

The rest of the paper is organized as follows: The related work is presented in the section II, the proposed work is discussed in the section III, the simulation experimental results and discussion are presented in the section IV, and the conclusion is given in the section V.

II. RELATED WORK

A modified AODV with dynamic wormhole detection and prevention has been proposed in [1] which is based on a hybrid model that encapsulates location, neighbor node and hop counts. A distributed synchronizing system based on logical clocks that order the events is described in [2]. In [3], time-stamping the events in both synchronous and asynchronous message passing programs that preserve the partial ordering inherent in a parallel system is discussed. Secured message transmission in MANETs through identification and removal of byzantine wormhole attack by selecting secured routes in active path set (APS) is discussed in [4]. Investigation and analysis of wormhole and blackhole attacks prevention methods in MANETs is carried out in [5]. In [6], an adaptive fuzzy inference system is proposed for detection and prevention of cooperative blackhole attack in MANETs, which is compared with adaptive method. The fuzzy logic system shows better performance as compared to adaptive method in terms of throughput, end-to-end delay and packet delivery ratio. A survey of routing attacks and counter measures is presented in [8], wherein the methods are classified into three classes, namely, solutions based on cryptography, intrusion detection systems and trust management and reputation–based solutions. In [9], the solutions to detect and prevent DoS attacks on network layer, namely, wormhole attack, blackhole attack and grayhole attack which are serious threats in MANETs are discussed. In [10], secured routing protocols are classified into three categories: solutions based on cryptography, solutions based on one-way hash chain and hybrid solutions and also comparison of various protocols available for secured routing in MANET is given. But very few of them are found to reduce the overhead and complexity of the network. A reliable solution for the problem of packet dropping attack by malicious nodes is developed in [11], using fuzzy logic. In [12], a secured transmission in MANETs with wormhole and blackhole attacks is addressed using fuzzy inferencing. A reliable multipath communication in MANETs affected by wormhole and blackhole nodes is proposed in [13] using Lamport timestamp algorithm (LTAWB). The literature survey reveals that there is a need for development of an efficient method to detect and prevent wormhole and blackhole attack in MANETs by reducing the complexity and overhead cost. In the present paper, the aim of the proposed method is to detect and prevent wormhole and black hole attack using LTAWB technique with fuzzy inference system to detect the malicious behaviour of nodes.

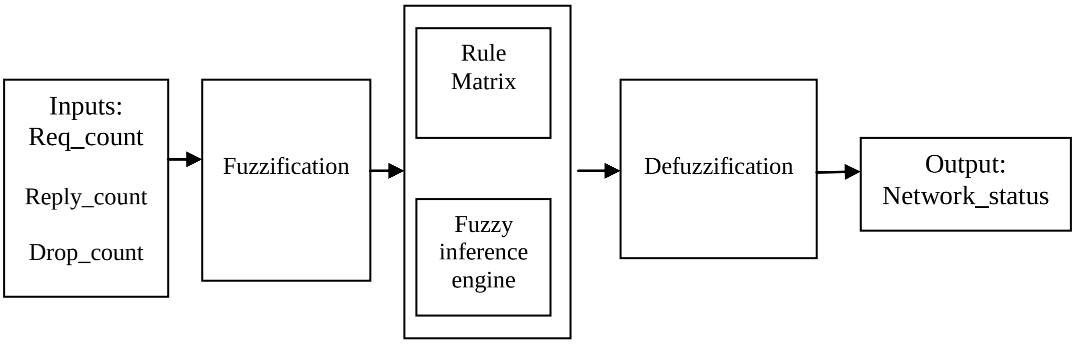

Figure 3. Model of fuzzy inference system

III. Proposed work

The proposed method for detection and prevention of both the attacks, namely, blackhole and wormhole, is based on the Lamport timestamp algorithm which reduces the complexity and the overhead of the network. A fuzzy inference system is incorporated with Lamport timestamp algorithm to improve the performance in terms of detection of malicious nodes. The proposed methodology is described below.

A. *Fuzzy inference system (FIS)*

The fuzzy logic simulates human decision making process by allowing the use of imperfect information in a most sensible way. Also, fuzzy logic can be implemented in hardware, software, or a combination of both. A fuzzy logic based fuzzy inference system is designed using four main elements, namely, fuzzification interface, fuzzy inference engine, fuzzy rule matrix and defuzzification interface. The block diagram of the proposed FIS is shown in the Fig.3.

Fuzzification

The input parameters of the inference system are considered as fuzzy variables with linguistic hedges as values. These parameters are represented by pre-defined input membership functions, e.g. triangular shape, Gaussian, trapezoidal, sinusoidal and exponential. In this work, triangular membership functions are used for three input variables, namely, Req_count, Rep_count and Drop_count and a single constant output variable is Network_status. The Network_status is any one of the three constant values, namely, 0.4 (LOW), 0.6 (MED) and 1.0(HIGH). The Network_status LOW indicates that the node is suspected to be malicious. The Network_status indicates the availability of resources in terms of energy and bandwidth. The Network_status value LOW indicates, the node has low resources. The Network_status value MED indicates, the node has fairly good resources and if the Network_status value is HIGH, it indicates the node has high resources. Therefore, the Network_status with MED is selected as the best next-hop neighbor, due to the average or medium level resources are available for the respective node, this node will be considered as genuine node or normal node. There is only one output variable. Its value has linguistic hedges: LOW, MED and HIGH. The linguistic hedges for input and output variables are LOW, MED and HIGH with the weights as defined in the Tables I and II.

B. *Rule matrix*

The rule matrix is used to describe fuzzy logic in the form of conditional statements. A fuzzy if-then rule framed in this work has the general form as, If x is A then y is Z, where, A is a set of conditions that have to be satisfied by inputs and Z is a set of consequences (outputs) that can be inferred. In a rule with multiple parts, fuzzy operators (AND, OR, NOT) are used to combine more than one input. The fuzzy rules used in proposed system are given in Table III. The if_then rules formed on the basis of Table III are given below.

Some sample if-then-rules used in the proposed inference system are given below and entire set of if-then rules is given in the Table III.

Rule 1: IF (Req_count = = MED AND Rep_count = = HIGH AND Drop_count = = LOW) THEN Network_status = LOW.

Rule 2: IF (Req_count = = MED AND Rep_count = = LOW AND Drop_count = =HIGH) THEN Network_status = HIGH.

Rule 3: IF (Req_count = = MED AND Rep_count = = MED AND Drop_count = =LOW) THEN Network_status = MED.

C. *Fuzzy inference engine*

The fuzzy inference mechanism allows mapping the given input to an output using fuzzy logic. It uses pre-defined fuzzy membership functions, logical operations and if-then rules. The most common types of inference systems are Mamdani and Sugeno models which vary in the ways of determining outputs. In Mamdani model, it is expected that the output is a fuzzy set and, in Sugeno model, the output is expected to be linear or constant. In the proposed work, Sugeno model is employed, since the nature of problem in hand expects a constant output for a set of inputs.

D. *Defuzzification*

The output is a fuzzy value, which needs to be defuzzified, i.e. mapped to a crisp value, for inferencing. The defuzzification task is performed by one of the mathematical techniques, namely centroid, bisector, fuzzy mean, maximum, maximum and weighted average. In the proposed work, fuzzy mean method for defuzzification is employed.

E. *Fuzzy Lamport Timestamp Algorithm (FLTA)*

The proposed methodology employs Fuzzy LTA for packet filtering pertaining to wormhole and blackhole attacks in MANETs. Lamport was the first to give a distributed mutual exclusion algorithm by illustrating to clock synchronization scheme. Timestamp of Req_Count, Rep_Count, Drop_Count and update time are maintained in the Lamport list. Time stamp value of two events is compared and is validated in sequential order. If the events are not in the form of sequential order, then the sorting of events based on timestamp is performed. The timestamp ordering is executed by comparing three consecutive events and are sorted in ascending order. Again, the timestamp ordering is executed by comparing two consecutive events and sorted in ascending order. Once the timestamp ordering is completed, fuzzy system is invoked by taking the current event and its timestamp as input to the fuzzy process. The timestamp input of request, reply and drop counts are given as input to the fuzzy inference system. The inputs are normalized by dividing maximum value and ranged between 0 and 1. The lower boundary and upper boundary of each input is compared and marked as linguistic variable, namely, LOW, MED and HIGH. The rule set is matched by validating three input variables and matched output is derived as LOW, MED and HIGH. Output rule is matched and defuzzification is applied to derive the value between 0 and 1. The lower boundary for defuzzified output is derived from lower boundary of three fuzzified values. If the obtained output rule value is less than lower boundary of defuzzified output, then the detection is done by validating the Lamport timestamp value and its corresponding event. The events, which are not sorted in the given order are isolated as abnormal events with respect to the timestamp, and such isolated events are classified as event action performed by the malicious behavior of the nodes related to such events. The proposed method is presented in the form of the following algorithm.

Algorithm:

Let N be no. of nodes in the MANET and x be the percentage of blackhole and wormhole nodes, S is the source node. Time stamp value and its corresponding event values are maintained as T and C.

```
Step 1: Input the values of N and x.
Step 2: Randomly assign x% nodes as black hole and
        wormhole nodes among N nodes.
Step 3: The route discovery is initiated by S by periodically
        broadcasting HELLO packet and update neighbor
        links.
Step 4: Timestamp of the Request packet count (Req_count),
        Reply packet count (Rep_count) and packet Drop
        count (Drop_count) are maintained in the Lamport
        list.
Step 5: Time stamp value of two events are compared and it is
        validated for sequential order.
Step 6:If the events are not in the sequential form, then the
        sorting of events based on timestamp is performed.
Step 7: The timestamp ordering is executed by comparing
        three consecutive events and sorted in
        ascending process.
Step 8:Again, the timestamp ordering is executed by
        comparing two consecutive events and sorted in
        ascending process.
Step 9: Upon completion of timestamp ordering, fuzzy process
        is invoked by taking the current
        event and its timestamp as input to the fuzzy process.
Step 10: Timestamp of Req_count, Rep_count and Drop_
         count are given as input to the fuzzification.
         The input is normalized by dividing maximum value
         and ranged between 0 and 1.
Step 11: Depending upon the input condition the
         Network_status is evaluated as LOW, MED or HIGH.
Step 13: The defuzzification is applied to fuzzy output.
Step14: A node is selected for further routing when
         Network_status value is MED ( because at MED the
         network parameters are in acceptable range (Figs.
         16-21). If Network_status value is either LOW or
         HIGH, the node will be treated as malicious and
         rejected for routing.
Step 15: Compute the performance metrics, which includes,
         throughput, packet delivery ratio and end- to- end
         delay.
Step 16: Stop.
```

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The simulation experiments of the proposed algorithm (FLTA) are conducted using NS-2.34 simulator with the simulation parameters chosen as mentioned in the Table IV. The efficiency of the proposed Fuzzy Lamport Timestamp algorithm (FLTA) is analyzed on the basis of three performance metrics, namely, throughput, packet delivery ratio and end-to-end delay, in the presence of different percentage of blackhole nodes (1%, 2%,3%, 4%, and 5%) and wormhole nodes (2%, 4%,6% and 8%) in a MANET having 100 nodes. The results are compared with that of the LTAWB [13] and SMTWB [12].

Throughput: It is a measure of how many data packets are transmitted from source to destination in a given amount of time and is represented in bits per second (bps). It is observed in Fig.4 that, as the number of blackholes nodes increases, throughput continues to be decreased. It is noticed in Table V, that there is significant improvement in throughput due to proposed FLTA. The throughput is increased by 14.5% by using the proposed algorithm FLTA, in comparison with that of LTAWB method in [13], and in the presence of blackhole attack with 1% of nodes as blackhole nodes. With the rise in concentration of blackholes, there is reduction in performance of network. It is observed in Fig.7 that, as the density of wormhole nodes increases, throughput continues to be decreased. In the Table VI, it is noticed that the throughput is increased by 17.4% by using the proposed FLTA, in comparison with that of LTAWB method in [13], in the presence of 2% of nodes as wormhole nodes. The throughput is increased by 32% by using the proposed FLTA, in comparison with SMTWB protocol [12], in presence of 1% of nodes as blackhole nodes. With the rise in concentration of blackholes, there is reduction in performance of network as shown in Fig.13 and Table V. It is noticed in Fig.10 that, as the density of wormhole nodes increases, throughput continues to be decreased. In the Table VI, it is observed that the throughput is increased by 44.3% by using the proposed FLTA, in comparison with that of SMTWB protocol [12], in the presence of 2% of nodes as wormhole nodes.

Packet Delivery Ratio (PDR): It is the ratio of data packets that are successfully delivered to a destination compared to the number of packets that have been transmitted by sender. It is observed in Fig.5 that, as the density of blackhole nodes increases, PDR continues to be decreased. For 1% of blackhole nodes, PDR increases by 6% by using the proposed algorithm FLTA, in comparison with that of LTAWB method in [13] as illustrated in Table V. As depicted in Fig.8, as the density of wormhole nodes increases, PDR continues to be decreased. For 2% of wormhole nodes, PDR increases by 5.4% by using the proposed algorithm FLTA, in comparison with that of LTAWB method in [13] as illustrated in Table VI. It is observed from the Fig.11 and Table VI that the PDR is increased by 36.4% by using the proposed FLTA, in comparison with SMTWB protocol [12], in presence of 2% as wormhole nodes. With the rise in concentration of wormholes, there is reduction in performance (PDR) of network. The PDR is increased by 32% by using the proposed FLTA, in comparison with SMTWB protocol [12], in presence of 1% as blackhole nodes. With the rise in concentration of blackholes, there is reduction in performance (PDR) of network as shown in Fig.14 and Table V.

End to end delay: The sum of time taken by data packets to reach effectively from source node to a destination is called as end-to-end (E2E) delay. It is observed from Fig.6 and Table V that, the delay is reduced by using proposed FLTA. The end-to-end delay is decreased by 28.6% by using the proposed algorithm FLTA, in comparison with that of LTAWB method, in the presence of blackhole attack with 1% of nodes as blackhole nodes. It is observed in Fig.6 and Fig.9 that, as the density of blackhole and wormhole nodes increases, end-to-end delay increases for both LTAWB[13] and the proposed FLTA. The overall performance of FLTA is better when compared with LTAWB. It is observed from the Fig.12 and Table V that the end-to-end delay is decreased by 85% by using the proposed FLTA, in comparison with LTAWB[13], in presence of 1% as blackhole nodes. The end-to-end delay is decreased by 69% by using the proposed FLTA, in comparison with SMTWB protocol [12], in presence of 5% as blackhole nodes as depicted in Table V. Also, the end-to-end delay is decreased rapidly in comparison with SMTWB [12] as shown in Fig.15 and Table VI in presence wormhole nodes.

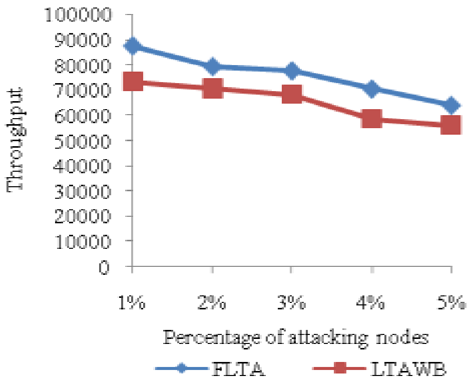

Figure 4. Throughput for varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: Comparison after filtering of blackhole packets using proposed FLTA and LTAWB[13].

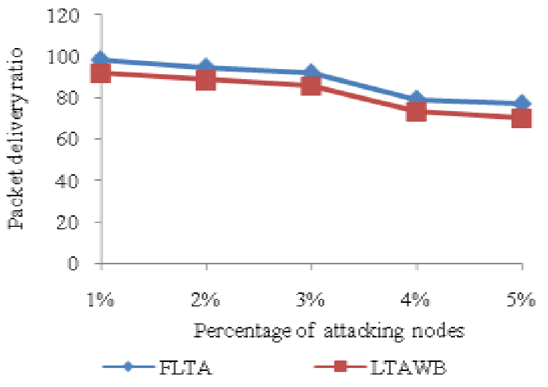

Figure 5. Packet delivery ratio for varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: Comparison after filtering of blackhole packets using proposed FLTA and LTAWB[13].

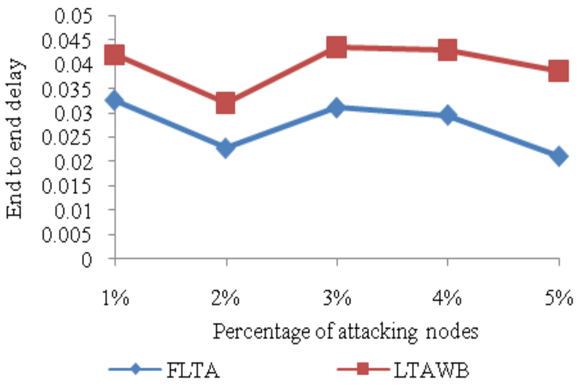

Figure 6. End-to-end delay for varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: Comparison after filtering of blackhole packets using proposed FLTA with LTAWB[13].

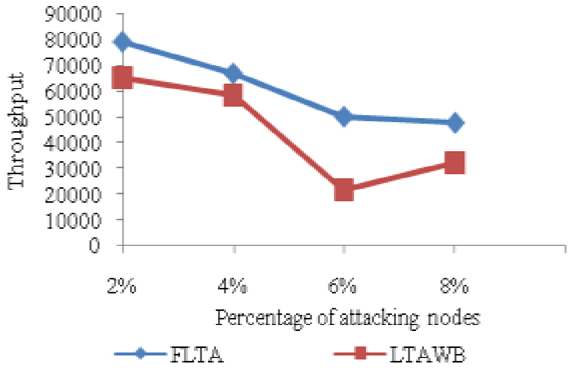

Figure 7. Throughput for varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: Comparison after filtering of wormhole packets using proposed FLTA and LTAWB[13].

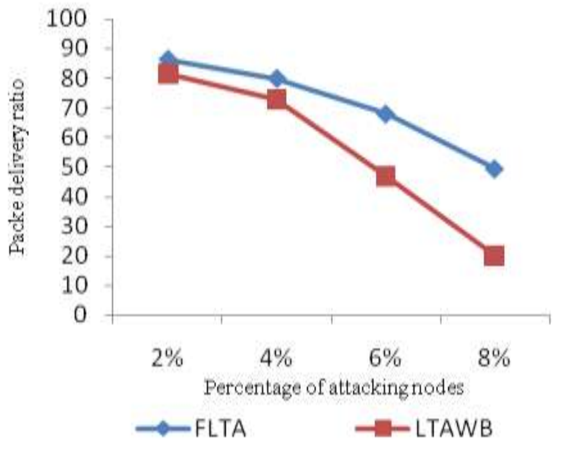

Figure 8. Packet delivery ratio for varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: Comparison after filtering of wormhole packets using proposed FLTA and LTAWB[13].

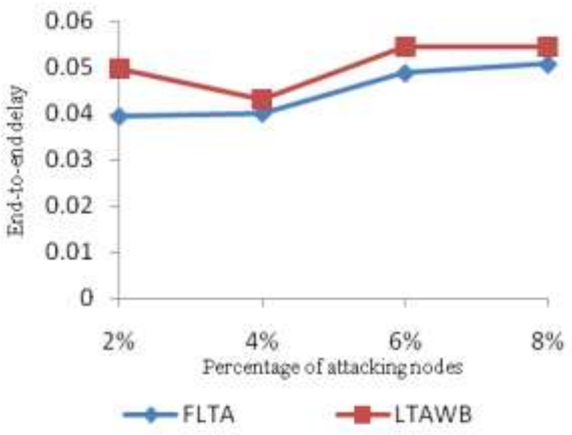

Figure 9. End-to-end delay for varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: Comparison after filtering of wormhole packets using proposed FLTA with LTAWB[13].

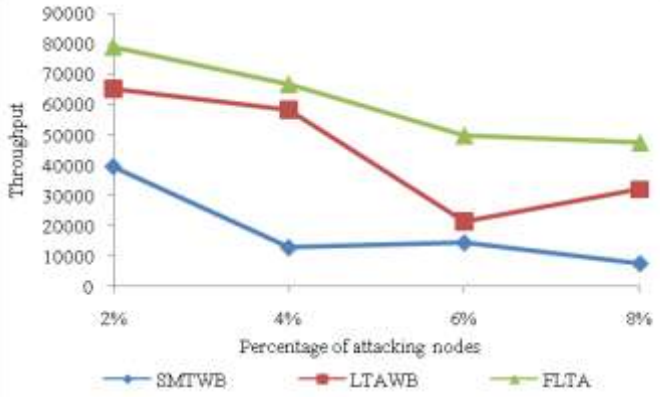

Figure 10. Throughput for varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: Comparison after filtering of wormhole packets using proposed FLTA, SMTWB[12] and LTAWB[13].

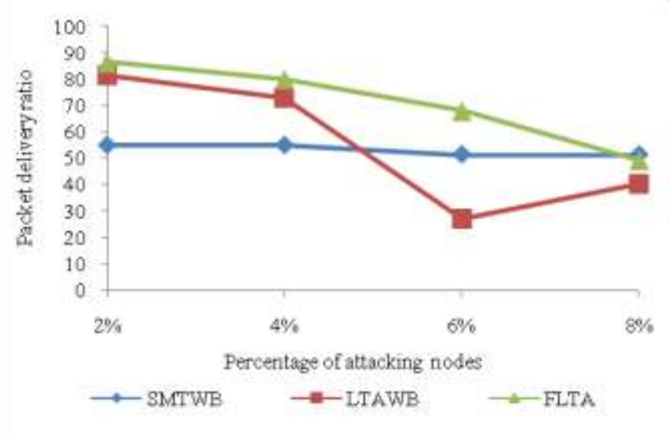

Figure11. Packet delivery ratio for varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: Comparison after filtering of wormhole packets using proposed FLTA, SMTWB[12] and LTAWB[13].

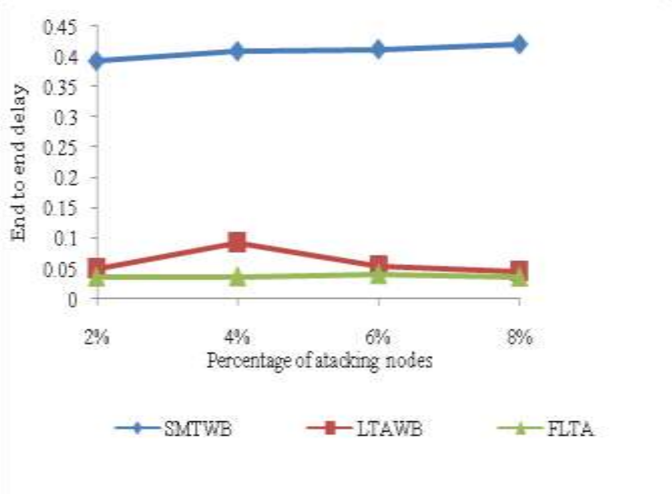

Figure 12. End-to-end delay for varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: Comparison after filtering of wormhole packets using proposed FLTA, SMTWB[12] and LTAWB[13].

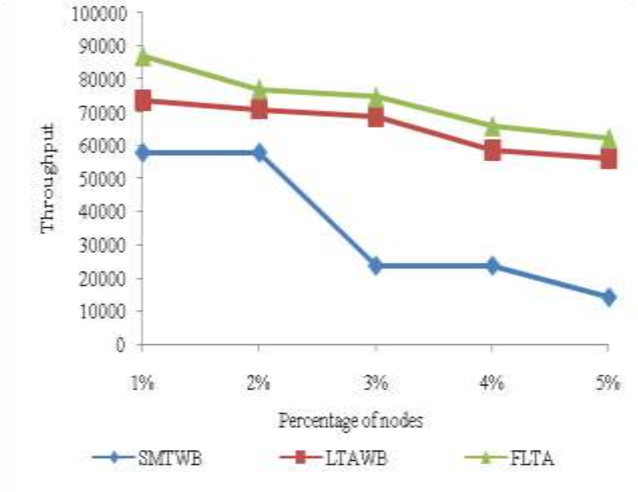

Figure 13. Throughput for varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: Comparison after filtering of blackhole packets using proposed FLTA, SMTWB[12] and LTAWB[13].

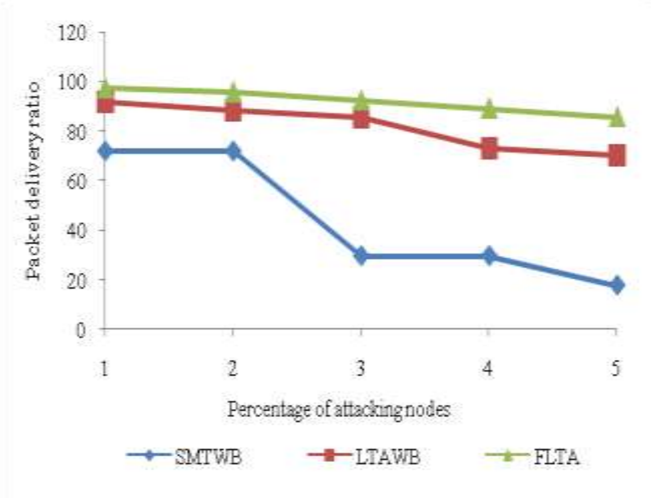

Figure 14. Packet delivery ratio for varying number of blackhole nodes x=1, 2, 3, 4 and 5%of N=100 nodes: Comparison after filtering of blackhole packets using proposed FLTA, SMTWB[12] and LTAWB[13].

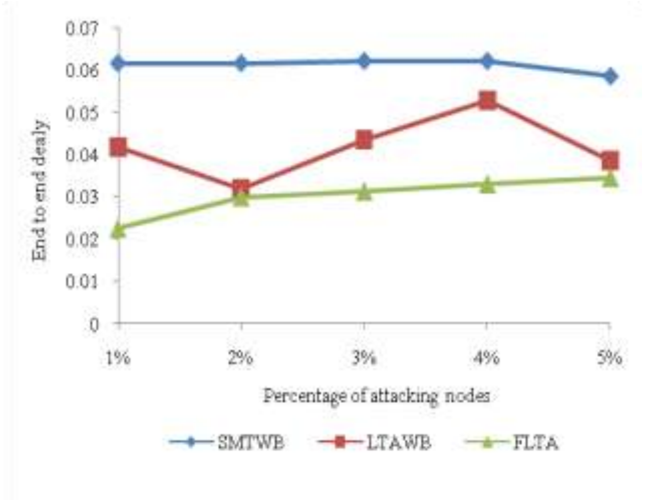

Figure 15. End to end delay for varying number of blackhole nodes x=1, 2, 3, 4 and 5%of N=100 nodes: Comparison after filtering of blackhole packets using proposed FLTA, SMTWB[12] and LTAWB[13].

A comparison of the network performance parameters namely, throughput, packet delivery ratio and end-to-end delay is performed. It is found that when the Network_status is MED. The network performance parameters like Throughput and PDR are high and end-to-end delay is low. This comparison is made in case of other two methods LTAWB and SMTWB in presence of blackhole and wormhole affected nodes and it is observed that the proposed method yields better results as shown in Figs. 16-21. Thus, the proposed Fuzzy Lamport Timestamp algorithm (FLTA) yields better results in comparison with the SMTWB[12] protocol and LTAWB[13]. As concentration of blackhole and wormhole node increases, the available paths are fewer which leads to further reduction in throughput and packet delivery ratio. The overall network performance indicates that the proposed Fuzzy Lamport Timestamp algorithm (FLTA) is more effective for detection and prevention of blackhole and wormhole attacks in MANETs.

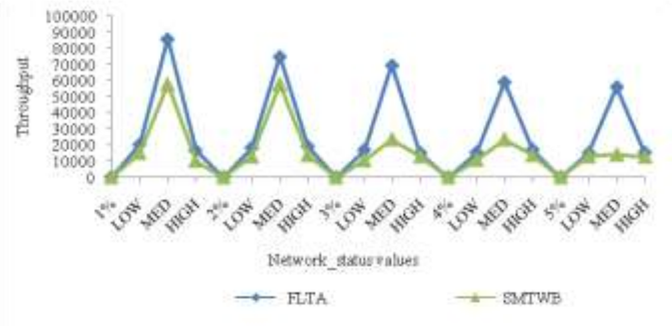

Figure 16. Throughput by varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: Network Performance Parameters at different Network_status (LOW, MED, HGH).

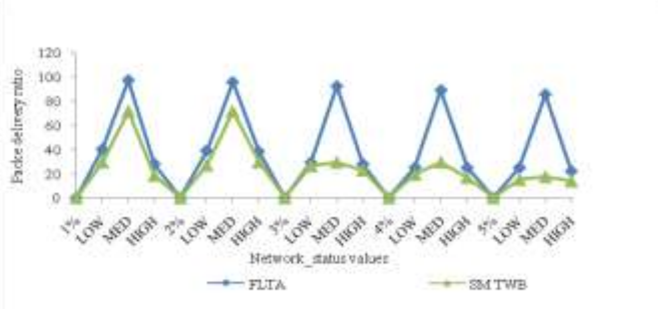

Figure17.Packet delivery ratio by varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: Network Performance Parameters at different Network_status (LOW, MED, HGH).

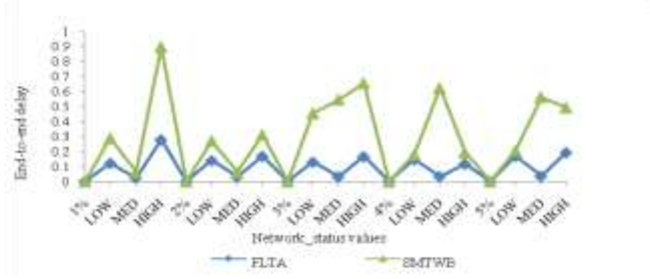

Figure 18. End-to-end delay by varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: Network Performance Parameters at different Network_status (LOW, MED, HGH).

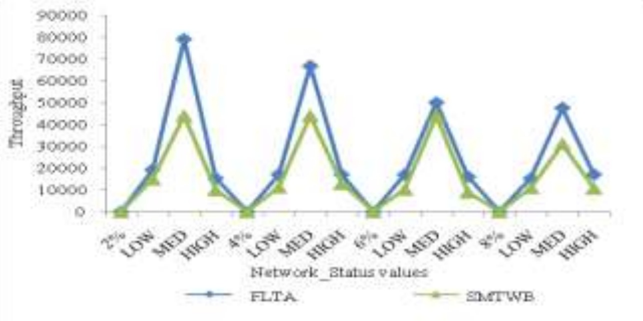

Figure 19. Throughput by varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: Network Performance Parameters at different Network_status (LOW, MED, HGH)

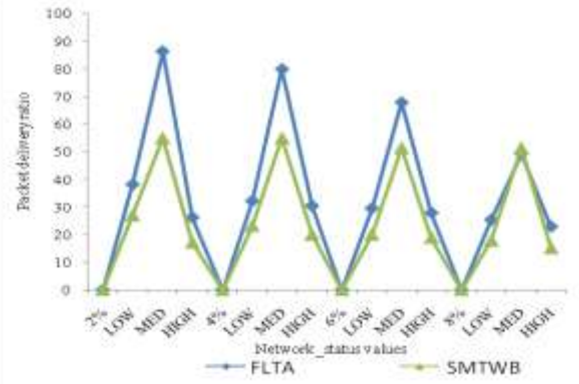

Figure 20. Packet delivery ratio by varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: Network Performance Parameters at different Network_status (LOW, MED, HGH)

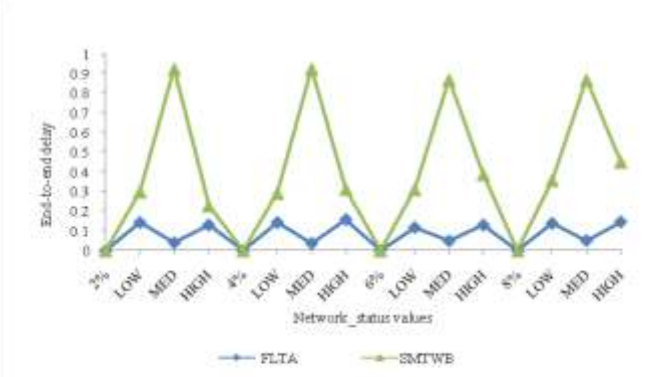

Figure 21. End-to-end delay by varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: Network Performance Parameters at different Network_status (LOW, MED, HGH)

V. CONCLUSION

In this paper, the Fuzzy Lamport timestamp algorithm (FLTA) is presented. It is used to identify the order of event and to make the synchronization of time clock in network devices. Each node performs monitoring process by Request message; Response message and packet drop action are monitored by the neighboring nodes; and, the corresponding clock time is noted by the monitoring node. This algorithm is tested for two types of attacks, namely, wormhole attack and blackhole attack, in MANETs. The FLTA deals with such applications more accurately because of its ordering of events by collecting the timestamps of these events and performs the ordering based on these events that is, its ability to produce the exact solution from fairly inaccurate information. Results of simulation experiments show that the proposed FLTA, yields better results when compared with LTAWB[13] and SMTWB[12] protocol. Also it is observed that by using FLTA for exclusion of wormhole and blackhole nodes, the performance of the network is improved in terms of three performance parameters, namely, throughput, packet delivery ratio and end-to-end delay, when compared with SMTWB and LTAWB. These results indicate that the proposed algorithm is more promising in detecting and preventing malicious attacks in MANETs and thereby, achieving better performance of MANETs.

Table I. Linguistic variables and values for input parameters

Input parameters	**Linguistic Variables**	**Weights defined for linguistic input variables**	**Type of membership functions used in proposed FLTA**

Req_count, Rep_count and Drop_count.	LOW, MED and HIGH	LOW=0 to 0.4
		MED=0.4 to 0.6
		HIGH=0.6 to 1.0
			Triangular membership functions for all inputs.

Table II. Linguistic variables and values for output variables

Fuzzy Output: Network_status values	**Weights defined for linguistic output variables**	**Type of membership functions used in proposed FLTA**
LOW/MED/HIGH	LOW 0.4, MED 0.6 and HIGH 1.0	Output function is a constant membership function.

Table III. Fuzzy rules table

SL.NO	Req_count	Rep_count	Drop_count	Network_status
1	LOW	LOW	LOW	MED
2	LOW	LOW	MED	HIGH
3	LOW	LOW	HIGH	HIGH
4	LOW	MED	LOW	LOW
5	LOW	MED	MED	LOW
6	LOW	MED	HIGH	HIGH
7	LOW	HIGH	LOW	HIGH
8	LOW	HIGH	MED	LOW
9	LOW	HIGH	HIGH	HIGH
10	MED	LOW	LOW	MED
11	MED	LOW	MED	HIGH
12	MED	LOW	HIGH	HIGH
13	MED	MED	LOW	MED
14	MED	MED	MED	MED
15	MED	MED	HIGH	HIGH
16	MED	HIGH	LOW	LOW
17	MED	HIGH	MED	HIGH
18	MED	HIGH	HIGH	HIGH
19	HIGH	LOW	LOW	LOW
20	HIGH	LOW	MED	LOW
21	HIGH	LOW	HIGH	HIGH
22	HIGH	MED	LOW	LOW
23	HIGH	MED	MED	MED
24	HIGH	MED	HIGH	HIGH
25	HIGH	HIGH	LOW	MED
26	HIGH	HIGH	MED	MED
27	HIGH	HIGH	HIGH	HIGH

Table IV. Simulation parameters and their values used in experimentation

Sl no	Parameters	Value
1	Packet size	512 bytes
2	Simulator	NS-2.34
3	Transmission range	250 mts
4	Node placement	Randomly
5	Number of black holes in terms of percentage	1%,2%,3%, 4% and 5% of total nodes
6	Number of worm holes in terms of percentage	1%, 2%,3%, 4% and 5% of total nodes
7	Simulation run time	100 sec to 500 sec
8	Number of Mobile Nodes	100 nodes
9	Topology	1000 * 1000 (m)
10	Routing Protocol	AODV
11	Traffic	Constant Bit Rate (CBR)

Table V. Comparison of throughput, packet delivery ratio (PDR), end-to-end (E2E) delay obtained by varying number of Blackhole nodes x=1, 2, 3, 4 and 5% of N =100 nodes for the proposed method FLTA with LTAWB[13] and SMTWB [12] protocols.

% of Blackhole nodes	**Throughput**			**PDR**			**E2E delay**		
	FLTA	**LTAWB [13]**	**SMTWB [12]**	**FLTA**	**LTAWB [13]**	**SMTWB [12]**	**FLTA**	**LTAWB [13]**	**SMTWB [12]**
1%	85885.2	73434.8	57714.3	97.56	91.7436	72.0571	0.02256	0.0418734	0.0616797
2%	74901.6	68196.7	57714.3	95.9	88.4302	72.0571	0.02995	0.0318883	0.0616797
3%	69524.6	62469.9	23714.3	92.52	85.497	29.6076	0.03134	0.0434649	0.0621764
4%	59027.3	54565.6	23714.3	89.25	73.1668	29.6076	0.033043	0.0528701	0.0621764
5%	561311	51130.4	14190.5	85.76	70.1249	17.717	0.034548	0.0385823	0.0585664

Table VI. Comparison of throughput, packet delivery ratio(PDR) and end-to-end (E2E) delay obtained by varying number of Wormhole nodes x=2, 4, 6 and 8% of N=100 nodes for the proposed method FLTA with LTAWB[13] and SMTWB[12] protocols.

% of Wormhole nodes	**Throughput**			**PDR**			**E2E delay**		
	FLTA	**LTAWB [13]**	**SMTWB [12]**	**FLTA**	**LTAWB [13]**	**SMTWB [12]**	**FLTA**	**LTAWB [13]**	**SMTWB [12]**
2%	79025.14	65217.4	44000.4	86.4297	81.4775	54.9346	0.0394281	0.0497585	0.925724
4%	66733.33	58347.8	44000.4	79.9711	72.8952	54.9346	0.0370746	0.0930731	0.925724
6%	49958.47	21434.8	41142.9	67.925	26.7789	51.3674	0.048817	0.054563	0.869923
8%	47584.1	32043.5	41142.9	49.3427	40.0326	51.3674	0.0507633	0.045423	0.869923

REFERENCES

[1] Neha Sahu, Deepak Singh Tomar and Neelam Pathak, “A Modified AODV Protocol to Detect and Prevent the Wormhole: A Hybrid Approach”, International Journal of Computer Science and Network Security (IJCSNS), Vol. 15, No. 2, 2015, pp. 115-118.

[2] Leslie Lamport, “Time Clocks, and the Ordering of Events in a Distributed System”, Communication of the ACM, Vol. 21, No. 7, 1978, pp. 558-565.

[3] Colin Fidge J, “Timestamps in Message –Passing Systems That Preserve the Partial Ordering”, Australian Computer Science Communications, Vol. 10, No. 1, February 1988, pp. 56-66.

[4] Anitha.V, J. Akilandeshwari, “Secured Message Transmission in Mobile Adhoc Networks through Identification and Removal of Byzantine Failures”, Inter Jl. Computer Science and Networking, Vol. 2, issue 1, August 2012, pp. 14-18.

[5] Dmitry Moskvin, Denis Ivanov, and Dmitry Zegjda, “Wormhole and Blackhole Attacks on Adhoc Networks Prevention Methods”, Advances in Information Science and computer Engineering, ISBN: 978-1-61804-276-7, pp. 180-184.

[6] Hiremath P.S, Anuradha T. and Prakash Pattan, “Adaptive Fuzzy Inference for Detection and Prevention of Cooperative Blackhole Attack in MANETs”, Proceedings of International Conference on Information Science (ICIS), 2016, pp. 198-203.

[7] Hiremath P.S, Anuradha.T and Prakash Pattan, “SMTWB-Secured MANET Transmission for Wormhole and Blackhole Attacks using Fuzzy Logic”, Proceedings of International Conference on Current Research and Applications in Electrical Sciences (ICCRAES), 2016, pp. 236-241.

[8] Amara korba Abdelaziz, Mehdi and Nafaa, Ghanemi Salim, “Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks”, Proceedings of 15th International Conference on Computer Modelling and Simulation, 2013 IEEE, pp. 693-697.

[9] Rutvij H.Jhaveri, Sankita J.Patel and Davesh C. Jinwala, “DoS Attacks in Mobile Ad-hoc Networks: A Survey”, Proceedings of International Conference on Advanced Computing and Communication Technologies, 2012 IEEE, pp. 535-541.

[10] Houda Moudni, Mohamed Er-rouidi,hicham Moucil, Benachir El Hadadi, “Secure Routing protocols for Mobile ad hoc Networks”, Proceedings of International Conference on Information Technology for Organizations Development (ITOD), 2016 IEEE, pp. 1-7.

[11] Alka.C, Tiwari.V.N and Anil kumar, “A Reliable Solution against Packet Dropping Attack due to Malicious Nodes Using Fuzzy Logic in MANETs”, International Conference on Reliability, Optimization and Information Technology (ICROIT), 2014, pp. 178-181.

[12] Hiremath P.S, Anuradha T. and Prakash Pattan, “SMTWB-Secured MANET Transmission for Wormhole and Blackhole Attacks using Fuzzy Logic”, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), Vol. 23 Issue 6, 2016, pp. 236-241.

[13] Hiremath P.S, Anuradha T. and Prakash Pattan, “LTA based Filtering of Wormhole and Blackhole node packets for Reliable Multipath Communication in MANETs”, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 5, Issue 12, 2016, pp. 501-508.

APPENDIX

A. Lamport Timestamp Algorithm

Lamport developed a notation that is express as a→ b, means that a happens before b. If a is the message being sent and b is a message been received, then a→b is true. Any message cannot be received before it is sent. Lamport has its own parameter called time synchronization, but apart from time synchronization in our work added the additional parameters like order of events and dropping ratio to detect and prevent the blackhole and wormhole attack in MANETs. Initially Lamport list is initialized as empty along with node id. The three parameter lists are used as c1, c2 and c3, where c1, maintains the count of control packets like RREQ, c2 maintains the count of RREP control packet and c3 maintains the count of drop count(number of packets dropped). The equality condition is applied between the neighboring nodes to check whether their RREQ count of i^{th} and j^{th} node is equal or not (i and j are the neighboring nodes). Similarly the greater than condition is also applied between the neighboring nodes. If the count of RREQ, RREP and drop count mismatches between the i^{th} and j^{th} nodes, then the attack is detected. Otherwise the count of RREQ and RREP and Drop count are said to be equal, then the node is said to be normal node All these three parameters are stored in Lamport list, with their respective count along with node id.
Illustrative numerical example of LTA for Manet in Fig.1

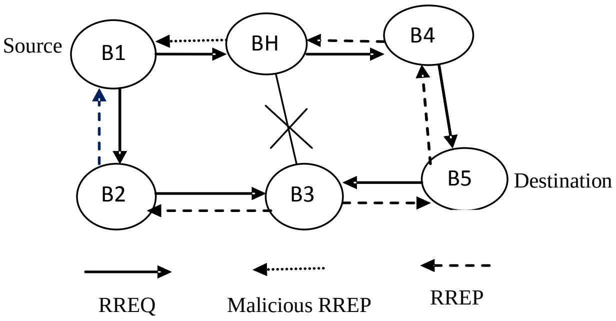

Figure 1.Blackhole attack in MANET

Events	Timestamp (TS)	From→node	Departure time(ms)	Arrival time(ms)	Output
Req_count=1 Reply_count=1 Drop_count=1 Network status=MED	TS=16.2012	B1→B2	10	25	Normal node
Req_count=2 Reply_count=4 Drop_count=5 Network status=LOW	TS=16.2152	B1→BH	10	5	Blackhole
Req_count=3 Reply_count=3 Drop_count=3 Network status=MED	TS=25.2296	B2→B3	25	39	Normal node
Req_count=4 Reply_count=8 Drop_count=5 Network status=HIGH	TS=05.0296	BH→B4	5	3	Blackhole
Req_count=5 Reply_count=10 Drop_count=6 Network status=LOW	TS=6.1228	BH→B3	6	4	Blackhole
Req_count=6 Reply_count=6 Drop_count=6 Network status=MED	TS=39.2291	B3→B5	39	100	Normal node

B. *Illustrative numerical example of LTA for MANET in Fig.2*

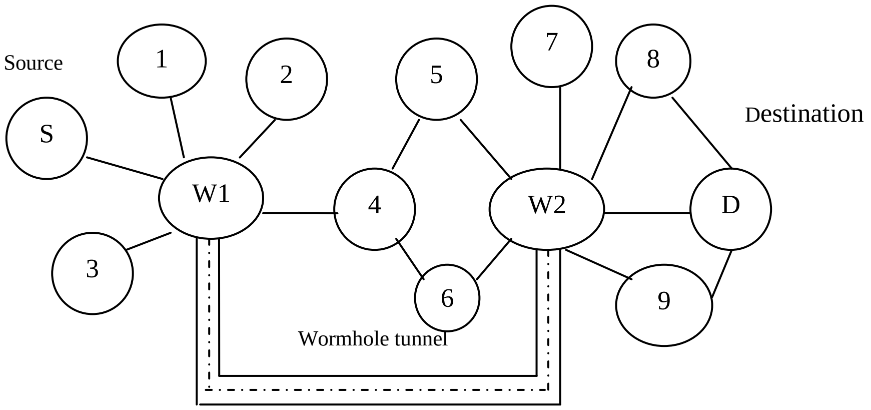

Figure. 2 Wormhole attack in MANET

Events	**Timestamp (TS)**	**From→node**	**Departure time(ms)**	**Arrival time(ms)**	**Output**
Req_count=1 Reply_count=1 Drop_count=1 Network_status =MED	TS=20.1012	S→W1	11	20	Normal node
Req_count=2 Reply_count=4 Drop_count=5 Network_status =HIGH	TS=26.2152	W1→4	20	10	Wormhole node
Req_count=3 Reply_count=3 Drop_count=3 Network_status= MED	TS=39.2296	4→6	10	39	Normal node
Req_count=4 Reply_count=4 Drop_count=4 Network_status =MED	TS=35.0296	4→5	11	35	Normal node
Req_count=5 Reply_count=10 Drop_count=6 Network_status =LOW	TS=19.1228	5→W2	35	19	Wormhole node
Req_count=6 Reply_count=10 Drop_count=8 Network_status =HIGH	TS=10.2291	W2→9	19	10	Wormhole node
Req_count=7 Reply_count=7 Drop_count=7 Network_status =MED	TS=90.0023	9→D	10	90	Normal node