IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

LTA based Filtering of Wormhole and Blackhole Node Packets for Reliable Multipath Communication in MANETs

P.S. Hiremath[1], Anuradha T[2], Prakash Pattan[3]

Dept of Computer Science (MCA), KLE Technological University, BVBCET, Hubballi, India[1]

Dept of Computer Science and Engg, PDA College of Engg, Kalaburagi, India[2, 3]

Abstract: A mobile ad-hoc network is a cluster of communication nodes which are capable of communicating among each other in the absence of a backbone. Due to increase in the use of wireless communication, minimizing the hindrances in wireless networks is becoming a high priority objective. Mobile ad-hoc wireless networks are vulnerable to wormhole and blackhole attacks. These attacks affect directly the performance of network. Prevention of such attacks on network is a challenging task. These attacks can result in a significant collapse of the wireless communication networks. In this paper, a novel method (LTAWB) based on LTA multipath routing is proposed, which filters the packets of wormhole and blackhole attacks, for reliable communication in MANETs. In the proposed method, LTA is used to identify the order of event and to make synchronization of time clock in network device that reduces the complexity. The simulated results of the proposed algorithm are compared with that of fuzzy logic based secured MANET transmission against wormhole and blackhole attacks (SMTWB)[7]. It is observed that the proposed LTAWB shows better performance as compared to SMTWB [7], in terms of throughput, end-to-end delay and packet delivery ratio.

Keywords: MANET, Wormhole, Blackhole, Lamport Timestamp Algorithm (LTA), AODV routing protocol, NS2 Simulator, Multipath routing, Security attacks.

1. INTRODUCTION

In mobile adhoc networks (MANETs), there is no centralized administration to take care of detection and prevention of attackers. A mobile ad-hoc network is a unique type of wireless network, in which group of mobile network interfaces may form temporary network without the aid of any established centralized coordinator. The main objective of MANET routing protocols are to maximize network throughput, enhance network lifetime, and minimize delay. Each node has communication capabilities. Nodes can directly correspond with each other if they are in radio coverage range of one another. Otherwise, nodes resort to multihopping, wherein each node behaves like station and router. All the nodes in the network participate routing and the network performance depends on the support between the nodes. MANETs are viable options, where infrastructure is absent or fixing is not possible. Security problems in a MANET are:

- Unlocked media
- Insecure routing protocols.
- Topology changes frequently.
- Central coordinator is non-existent.
- Cooperation is necessary between the devices.

MANET attacks can be classified as following:

A. Passive Attack: The purpose of passive attack is to snoop the confidential information for routing that should be kept secret during the communication. It obtains information without disturbing normal network operation. Such attacks are difficult to detect. (e.g., Traffic analysis, traffic monitoring and eaves dropping).

B. Active Attack: The purpose of active attack is to adapt the data being exchanged in the network. It may disrupt the regular functioning of the network. The intruders can alter the packets, inject the packets, drop the packet. Such attacks are very dangerous. (e.g., Modification, impersonation, fabrication, jamming and message replay). The Table 1 shows the various possible types of attacks occurring in different layers of a network protocol stack.

Table 1 Security Attacks on Different Layers of Protocol Stack

Layer	Types of Attacks
Application Layer	Repudiation, data corruption
Transport Layer	Session hijacking, SYN flooding
Network Layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks.
Data link Layer	Traffic analysis, monitoring, disruption MAC(802.11)

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Physical Layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the middle

The more frequently occurring security attacks, namely, wormhole and blackhole attacks, are described below.

C. Wormhole attack:

One of the most vigorous 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 attackers is referred as wormhole attack. Routing of packets can be disrupted when routing control messages are tunneled. The AODV routing protocol is considered to study the wormhole attacks. The 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, it presents an false impression of shortest path via wormhole nodes.

The Fig 1 depicts that there are six nodes: 'S' source node, 'D' destination node, w1 and w2 are the wormhole nodes which create the tunnel and allow the packets to move from one end (w1) to other end (w2), bypassing nodes 1 and 2. Hence, the packets are dropped without reaching the destination D.

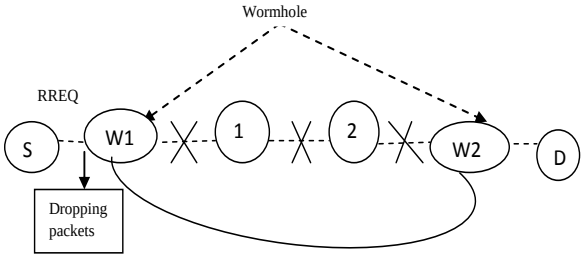

Fig.1. Wormhole attack in network.

D. Blackhole attack:

Among the various attacks in MANETs, blackhole is one of the severe attack. A blackhole is a wicked node that incorrectly replies for route requests. Without having an active route to the destination, it exploits the routing protocol to advertise itself as having a shortest route to desination. It is depicted in Fig.2. The node 1 is a source node and D is a destination node. Node BH (blackhole), node 2 and node 3 are the neighboring nodes of source node 1. When source node 1 sends a RREQ (Route Request) packet to its neighboring nodes, BH node replies immediately with RREP (Route Reply) packet to source node 1. In case, the response from the node BH reaches to node 1 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 1 or loses; finally, BH node becomes a black hole.

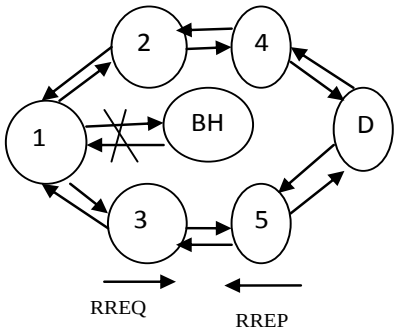

Fig.2. Blackhole attack in network

The rest of the paper is organized as follows: The related work is given in the Section II, the proposed work is described in the Section III, the simulation experimental outcomes along with the analysis of network performance parameters are presented in the Section IV and the conclusions are given in the Section V.

II RELATED WORK

In [1], a dynamic wormhole detection and prevention technique AODVWWDP (AODV with Wormhole Detection and Prevention) has been proposed which is based on hybrid model that encapsulates location, neighbor node and hop counts. A distributed algorithm is given for synchronizing a system of logical clocks which can be used to totally order the events [2]. An algorithm is presented in [3], for timestamping events in both synchronus and asynchronous message passing programs that allow for access to the partial ordering inherent in a parallel system. 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 are studied in [5]. In [6], an adaptive fuzzy inference system for detection and prevention of cooperative blackhole attack in MANETs, is proposed method and is compared with adaptive method. The fuzzy logic system shows better performance compared to adaptive method in terms of throughput, delay and packet delivery ratio. A protocol, SMTWB, has been proposed for secured transmission against wormhole and blackhole attacks in MANETs using fuzzy logic in [7]. A survey of countermeasures in a structured manner and having classified them into three classes: solutions based on cryptography, intrusion detection systems and trust management and reputation – based solutions, are studied in [8]. In [9], proposed 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], three categories of solutions: solutions based on cryptography, solutions based on one-way hash chain and hybrid solutions, are described and also a brief summary and comparison of various protocols available for secured routing in MANET are given.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

The literature study reveals that very few works have been able to reduce the overhead and complexity of the network. Further, in order to reduce the complexity and overhead of the network along with filtering packets of wormhole and blackhole attack using path randomization in MANETs, the LTA has scope in addressing the attacks of Blackhole and Wormhole attacks. The aim of the proposed method is to detect and prevent wormhole and black hole attack on the basis of LTA making use of collecting the timestamps of these events and then performing the ordering based on these events. Further, after processing imprecise or incomplete information about its neighboring nodes, the decision about the node to which data packets be transferred is taken.

III PROPOSED METHODOLOGY

The proposed methodology employs Lamport timestamping algorithm (LTA) for packet filtering in wormhole and blackhole attacks in MANETs. Lamport was the first to give a distributed mutual exclusion algorithm based on a clock synchronization scheme. Lamport has used the order of events in order to make synchronization of time clock in network devices. The timestamping process is applied for the monitoring of events and actions performed by the node. 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. The Lamport algorithm begins with the process of collecting the timestamps of these events and performs the ordering based on these events.

Whenever the events are initiated by the node, then current clock tick is incremented by 1 and the updated timestamp is attached in the message event. During the reception of the message event, timestamp of the receiver devices are synchronized with respect to the sender device as follows:

$$\text{Time} = \text{Max}(\text{time}, \text{timestamp}) \quad (1)$$

Once these events are collected for the events (including request, response and packet drop) count, verify the ordering of these events. The ordering is performed by comparing the timestamps of the node set. The clock time of the current event of one node in the Lamport list must not be equal to the time of the current event of another node. Also the timestamp must not be greater than other nodes' event timestamp. Whenever the clock tick is sorted, corresponding event also sorted with respect to the timestamp. Hence, the events of the nodes, which are not sorted in the given order, are isolated as abnormal events with respect to the timestamp. The isolated events are classified as the event action performed by the malicious behaviour of these nodes.

Algorithm:

Let N be the number of nodes and x be the % of blackhole and wormhole nodes. S is the source node.

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: The timestamping process is applied for monitoring events and actions performed by the node.

Step 5: Wireless network is deployed with a set of blackhole and wormhole nodes. Each node performs monitoring action. Request message, Response message and the packet drop actions are monitored by the neighboring nodes. The corresponding clock time is noted by the monitoring node.

Step 6: The Lamport algorithm begins with the process of collecting the timestamps of these events and performs the ordering based on these events.

Step 7: Whenever the events are initiated by the node then current clock tick is incremented by 1, and the updated timestamp is attached with the message event.

$$time = time + 1; \quad (2)$$

$$ch \rightarrow ts = time; \quad (3)$$

Step 8: During the receipt of the message event, timestamp of the receiver devices are synchronized with respect to the sender device as follows:

$$time = max(time, timestamp) + 1; \quad (4)$$

Step 9: Once these events (including Request, Response and Packet drop count) are collected, then verification and the ordering of these events begin. The ordering is performed by comparing the timestamps of the node set.

Step 10: The clock time of the current event of one node in the Lamport list must not be equal to clock time of another node. Also, the timestamp must not be greater than another node's event timestamp.

Step 11: Both validation are applied for all nodes to order the events based on the timestamp.

Step 12: Whenever the clock tick is sorted, corresponding event is also sorted with respect to the timestamp. This ordering process is executed by validating all clock events simultaneously in the first level.

Step 13: The events, which are not sorted in the order, are isolated as abnormal events with respect to the timestamp and correspond to malicious nodes' behavior..

Step 14: Compute the performance metrics, namely, throughput, packet delivery ratio and end to end delay.

Step 15: Stop.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The simulation experiments of the proposed algorithm are conducted using NS-2.34 simulator with the simulation parameters chosen as mentioned in the Table II.

The efficiency of the proposed LTA based method for wormhole and blackhole attack detection (LTAWB) is analyzed on the basis of three performance metrics,

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

namely, throughput, packet delivery ratio and end-to-end delay, in the presence of different percentage of black hole nodes (1%, 2%,3%, 4%, and 5%) and wormhole nodes (2%,4%,6% and 8%) in a network of total 100 nodes. The results are compared with that of the SMTWB [7].

Table II. SIMULATION PARAMETERS AND THEIR VALUES USED IN EXPERIMENTATION

Parameters	Value
Packet size	512bytes
Simulator	NS-2.34
Transmission range	250mts
Node placement	Randomly
Number of black holes in terms of percentage	1%,2%,3%, 4% and 5% of total nodes
Number of worm holes in terms of percentage	2%,4%,6% and 8% of total nodes
Simulation run time	100sec to 500sec
Number of Mobile Nodes	100 nodes
Topology	1000 * 1000 (m)
Routing Protocol	AODV
Traffic	Constant Bit Rate (CBR)

Throughput: It is a measure of how many data packets of information a system can process in a given amount of time and is represented in bits per second (bps). It is observed in Fig.3 that, as the number of blackhole nodes increases, throughput continues to be decreased. It is shown in Table 3, that there is improvement in performance due to packet filtering of wormhole and blackhole attack using proposed LTAWB. The throughput is increased by 75% by using the proposed algorithm (LTAWB), in comparison with that of SMTWB method in [7], in the presence of black hole attack with 5% of nodes as blackhole nodes. With the rise in concentration of black holes, there is reduction in performance of network. It is observed in the Fig.6 that, as the number of wormhole nodes increases, throughput continues to be decreased. The throughput is increased by 76% by using the proposed algorithm (LTAWB), in comparison with that of SMTWB method in [7], in the presence of wormhole attack with 8% of nodes as wormhole nodes as shown in Table 4 below.

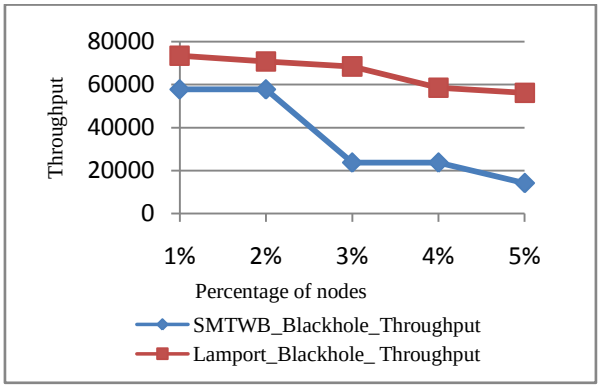

Fig. 3. Throughput for varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: After filtering blackhole packets using proposed LTAWB as compared to SMTWB [7].

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 sent out by sender. It is observed in Fig.4 that, as the number blackhole nodes increases, PDR continues to be decreased.

PDR increases by 21.4% by using the proposed algorithm (LTAWB), in comparison with that of SMTWB method in [7] as illustrated in Table 3. As depicted in Fig.7, when the number of wormhole nodes increases, PDR continues to be decreased. PDR increases by 39.33% by using the proposed algorithm (LTAWB), in comparison with that of SMTWB method in [7], as illustrated in Table IV.

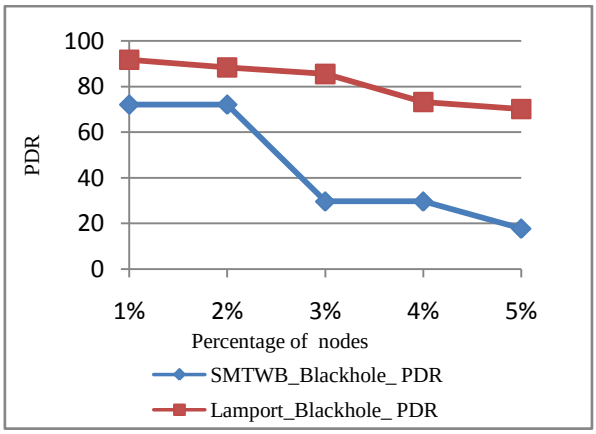

Fig. 4. Packet delivery ratio for varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: After filtering of blackhole packets using proposed LTA is compared with SMTWB protocol [7].

End to end delay: The sum of time taken from source node to transport the data packets effectively to a destination is called as End to End delay. The formula used to calculate the end to end delay is given by equation .

$$Delay = \frac{\sum(arrive\ time - send\ time)}{\sum Number\ of\ links} \quad \cdots \quad (5)$$

It is observed from Fig.5 and Table 3 that, the delay is reduced by using proposed algorithm based on LTA (LTAWB). The end to end delay is decreased by 52% by using the proposed algorithm (LTAWB), in comparison with that of SMTWB method[7], in the presence of black hole attack with 5% of nodes as blackhole nodes as shown in Table 3.

It is observed in Fig.8 that, as the number of wormhole nodes increases, end to end delay decreases rapidly by using the proposed algorithm (LTAWB), in comparison with that of SMTWB method in [7], in the presence of worm hole nodes as shown in Table IV.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

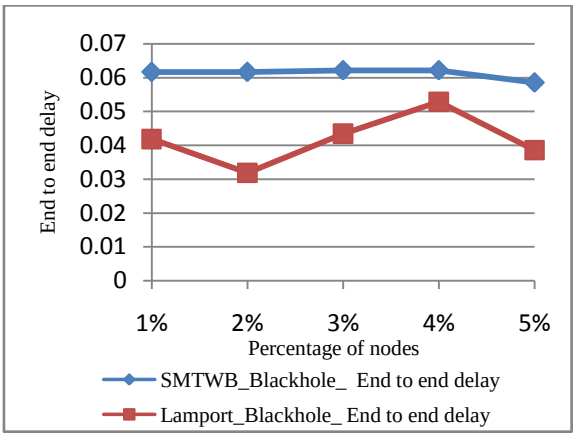

Fig.5. End to end delay for varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: After filtering blackhole packets using proposed LTAWB as compared to SMTWB [7].

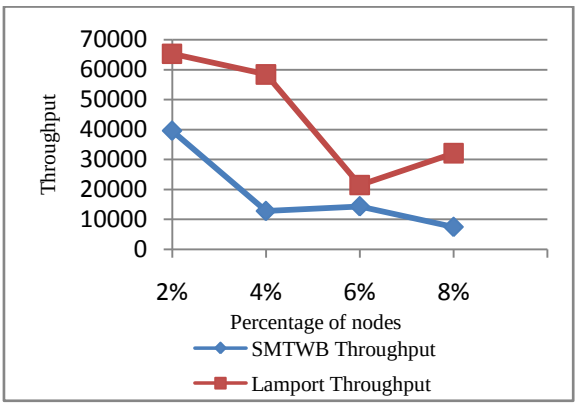

Fig. 6. Throughput for varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: After filtering wormhole packets using proposed LTAWB as compared to SMTWB [7].

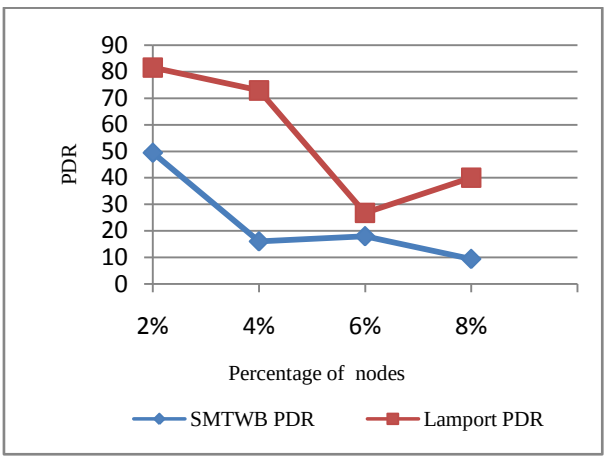

Fig. 7. Throughput for varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: After filtering wormhole packets using proposed LTAWB as compared to SMTWB [7].

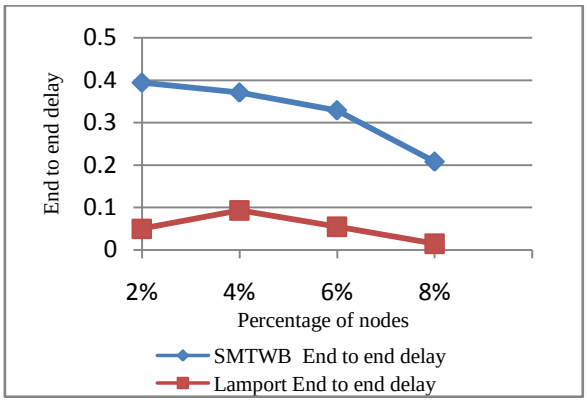

Fig.8. Throughput for varying number of wormhole nodes x=2, 4, 6 and 8% of N=100 nodes: After filtering wormhole packets using proposed LTAWB as compared to SMTWB [7].

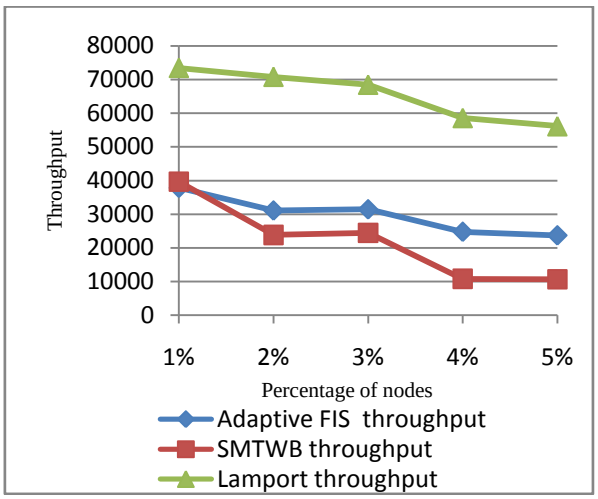

Fig. 9. Comparison of the three algorithms: Adaptive FIS, SMTWB and LTAWB for Throughput by varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: After detection and prevention of blackhole attack.

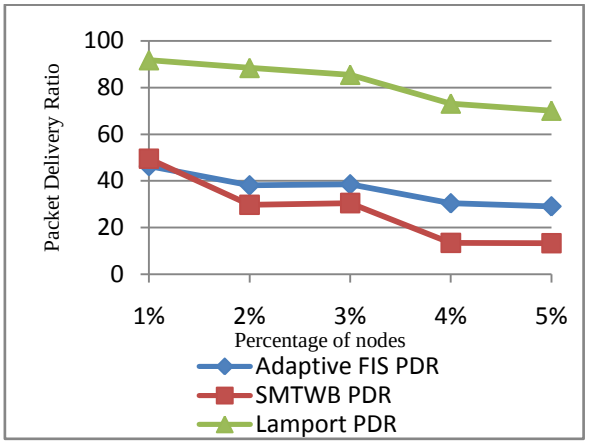

Fig. 10. Comparison of the three algorithms: Adaptive FIS, SMTWB and LTAWB for Packet Delivery Ratio by varying number of blackhole nodes x=1, 2, 3, 4 and 5% of

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

N=100 nodes: After detection and prevention of blackhole attack.

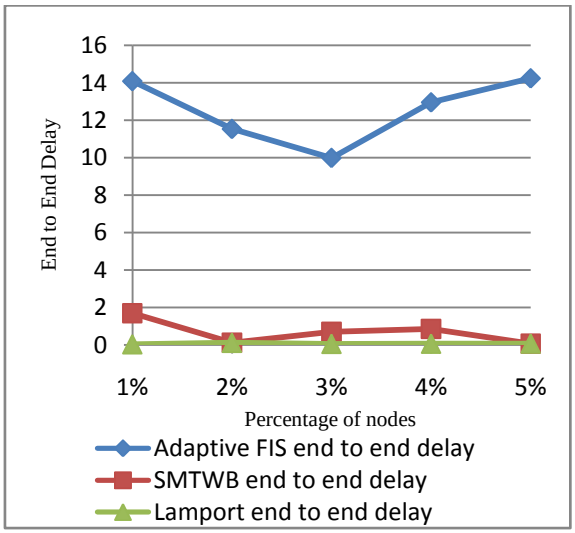

Fig. 11. Comparison of the three algorithms: Adaptive FIS, SMTWB and LTAWB for end to end delay by varying number of blackhole nodes x=1, 2, 3, 4 and 5% of N=100 nodes: After detection and prevention of blackhole attack.

The performance comparison of the three detection and prevention techniques, namely, proposed LTAWB, SMTWB[7], adaptive FIS[6], are depicted in Figs. 9-11, and also illustrated in Table 5 for blackhole attack. In [6], the adaptive FIS is developed for blackhole attack detection and prevention. Among these three algorithms, the proposed LTAWB method shows better results in comparison with the remaining two methods, namely, adaptive fuzzy inference system[6] and SMTWB[7]. Therefore, the overall network performance analysis implies that the complexity and overhead is reduced by using the proposed method based on LTA for detection and prevention of blackhole attack in MANETs.

V. CONCLUSION

The proposed method LTAWB based on Lamport timestamp algorithm (LTA) is used to identify the order of events 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 that are monitored by the neighboring nodes. The corresponding clock time is noted by the monitoring node. This algorithm is tested for both the attacks namely, wormhole attack and blackhole attack, in MANETs. The simulation experimental results are compared with that of SMTWB [7]. The LTA 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. Results of simulation experiments show that the proposed LTAWB, which uses the Lamport timestamp algorithm, yields better results for wormhole attack and blackhole attack, when compared with SMTWB [7]. These results indicate that the proposed algorithm is more promising in effectively and competently detecting and preventing different types of attacks in MANETs.

Table III. COMPARISON OF THROUGHPUTS, PDR AND E2E DELAY OBTAINED BY VARYING NUMBER OF BLACK HOLE NODES X=1, 2, 3, 4 AND 5% OF N=100 NODES FOR THE PROPOSED METHOD LTAWB AND SMTWB [7] PROTOCOL.

% of nodes Black hole	Throughput		PDR		E2E delay	
	SMTWB	Proposed LTAWB	SMTWB	Proposed LTAWB	SMTWB	Proposed LTAWB
1%	57714.3	73434.8	72.0571	91.7436	0.0616797	0.0418734
2%	57714.3	70782.6	72.0571	88.4302	0.0616797	0.0318883
3%	23714.3	68434.8	29.6076	85.497	0.0621764	0.0434649
4%	23714.3	58565.2	29.6076	73.1668	0.0621764	0.0528701
5%	14190.5	56130.4	17.717	70.1249	0.0585664	0.0385823

Table IV. COMPARISON OF THROUGHPUTS, PDR AND E2E DELAY OBTAINED BY VARYING NUMBER OF WORM HOLE NODES X=2, 4, 6 AND 8% OF N=100 NODES FOR THE PROPOSED METHOD LTA WITH SMTWB [7] PROTOCOL

% of nodes worm hole	Throughput		PDR		E2E delay	
	SMTWB	Proposed LTAWB	SMTWB	Proposed LTAWB	SMTWB	Proposed LTAWB
2%	39565.2	65217.4	49.4297	81.4775	0.925724	0.0497585
4%	12787.1	58347.8	15.9711	72.8952	0.869923	0.0930731
6%	14347.8	21434.8	17.925	26.7789	0.328817	0.054563
8%	7478.26	32043.5	9.34275	40.0326	0.207633	0.045423

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Table V. COMPARISON OF THE ADAPTIVE FIS[6], SMTWB[7] AND PROPOSED LTAWB FOR THE PARAMETERS THROUGHPUT, PACKET DELIVERY RATIO AND END TO END DELAY BY VARYING NUMBER OF BLACKHOLE NODES X=1, 2, 3, 4 AND 5% OF N=100 NODES: AFTER DETECTION AND PREVENTION OF BLACKHOLE ATTACK.

% of nodes blackhole	Throughput		
	Adaptive FIS [6]	**SMTWB [7]**	**Proposed LTAWB**
1%	37784.3	39608.7	73434.8
2%	31043.5	23782.6	70782.6
3%	31398.3	24391.3	68434.8
4%	24746.1	10739.1	58565.2
5%	23681.7	10608.7	56130.4
% of nodes blackhole	**PDR**		
	Adaptive FIS [6]	**SMTWB [7]**	**Proposed LTAWB**
1%	46.2792	49.484	91.7436
2%	38.0228	29.7121	88.4302
3%	38.4574	30.4726	85.497
4%	30.3096	13.4166	73.1668
5%	29.006	13.2537	70.1249
% of nodes blackhole	**E2E delay**		
	Adaptive FIS [6]	**SMTWB [7]**	**Proposed LTAWB**
1%	14.0884	1.69932	0.0418734
2%	11.5349	0.131083	0.118883
3%	9.9865	0.703956	0.0634649
4%	12.9552	0.867257	0.0728701
5%	14.2405	0.0744714	0.0785823

ACKNOWLEDGMENT

The authors are very thankful to the reviwers for their helpful comments which improves the quality of paper.

REFERENCES

[1] Neha Sahu, Deepak Singh Tomar and Neelam Pathak, "A Modified AODV Protocol to Detect and Prevent the Wormhole: A Hybrid Approach", IJCSNS International Journal of Computer Science and Network Security, vol 15 no 2, Feb 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, July 1978, pp 558-565.

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

[4] V. Anitha, Dr.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, pp14-18.

[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, pp180-184.

[6] P.S.Hiremath, 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, (In print)

[7] P.S.Hiremath, 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, (In print).

[8] Amara Korba Abdelaziz, Mehdi and Nafaa, Ghanemi Salim, "Suvey of Routing Attacks and Counter rmeasures 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 (IT4OD), 2016, IEEE, pp 1-7.

BIOGRAPHY

Dr. P.S. Hiremath, Professor (Retd), Department of P.G. Studies and Research in Computer Science, Gulbarga University, Gulbarga, Karnataka, India. Now, he is working in Department of Computer Science (MCA), KLE Technological University, Hubli. He has obtained M.Sc. degree in 1973 and Ph.D.degree in 1978 in Applied Mathematics from Karnatak University, Dharwad. He had been in the Faculty of Mathematics and Computer Science of various Institutions in India, namely, National Institute of Technology, Surathkal (1977-79), Coimbatore Institute of Technology, Coimbatore (1979-80), National Institute of Technology, Tiruchinapalli (1980-86), Karnataka University, Dharwad (1986-1993) and has been presently working as Professor of Computer Science in Gulbarga University, Gulbarga (1993 onwards). His research areas of interest are Computational Fluid Dynamics, Optimization Techniques, Image Processing and Pattern

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Recognition. He has published more than 150 research papers in peer reviewed International Journals and Proceedings of conferences.

Anuradha T, Assistant Professor, Department of computer Science and Engineering, P.D.A. College of Engineering, Gulbarga. She has obtained B.E (Computer Science and Engineering) degree in 2005 and M.Tech (Computer Science and Engineering) in 2007. She is pursuing her Ph.D. from Gulbarga University Kalaburagi. Her areas of interest are Computer Networking, Mobile Ad-hoc Network. She has published more than 12 research papers in peer reviewed International Journals and Proceedings of Conferences.

Dr. Prakash Pattan, System Manager (Prof), Department of Computer Science and Engineering, P.D.A. College of Engineering, Gulbarga, Karnataka, India. He has obtained M.Sc. (Information Technology) degree in 2003 and M. Tech. (Information Technology) degree in 2006. He has completed Ph.D. from Jawaharlal Nehru Technological University, Hyderabad in 2014. His research areas of interest are; Image Processing, Computer Networking and Pattern Recognition. He has published more than 25 research papers in peer reviewed International Journals and Proceedings of Conferences.