Detection of Misbehaving Nodes Using an Enhanced Acknowledgment Based Intrusion Detection Technique in MANETs

R.Jeyaawinothini[1], B.Leena[2], P.Gnanasundari[3]
PG Scholar[1, 2], Professor[3]
Department of Electronics and communication Engineering
SriGuru Institute of Technology, Coimbatore, Tamilnadu, India

Abstract- Mobile Ad hoc Network (MANET) is a collection of independent mobile nodes equipped with both wireless transmitter and receiver that communicate with each other via bidirectional wireless links either directly or indirectly within the same communication range. MANET is widely used in Military and Emergency recovery situations due to their self configuring capability. Since the nodes are widely distributed in MANETs, the malicious attackers can easily attack the entire system. Hence in order to overcome this problem, efficient Intrusion detection mechanisms have to be developed to protect MANETs from attacks. As the technology is being improved day by day, MANETs can be expanded to industrial applications and used effectively. So a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) is proposed and implemented. EAACK detects the malicious misbehavior of nodes better when compared to other techniques.

Keywords- Mobile Adhoc Network (MANET), Intrusion-detection System (IDS), Digital Signature, Enhanced Adaptive Acknowledgment (EAACK).

I. INTRODUCTION

Wireless networks are always preferred since the first day of their invention due to their natural mobility and scalability. An ad hoc network which is a decentralized type of wireless network is being used widely. The network is adhoc because it does not rely on a pre existing infrastructure instead each node participates in routing by forwarding data for other nodes, so the nodes forwarding data is based on the network connectivity used. An ad hoc network refers to set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. The basic principle behind adhoc networking is multi-hop relaying in which messages are sent from the source to destination by relaying through the intermediate hops. Hence due to the improved technology and cost reduction, wireless networks have more preferences over wired networks in the past few years.

One of the major classifications of Adhoc Networks is MANETs. By definition, a Mobile Adhoc Network is a collection of mobile nodes that communicate either directly or depending on other nodes as routers through wireless links. The operation of MANETs does not depend on an already existing infrastructure. In MANETs the network nodes move freely in random manner [8]. Therefore, the network topology of a MANET may change rapidly. The network activity like data packet delivery has to be executed by the nodes themselves, either individually or in a group. Based on its application, the structure of a MANET may vary from a static network to a dynamic network.

One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. But the problem is two nodes cannot communicate with each other when the distance between them is beyond their own communication range. MANET solves this problem by allowing intermediate nodes to relay data transmissions. So by dividing MANET into two types of networks, namely, single-hop and multihop this can be achieved. In a single-hop network, all nodes communicate directly with each other within the same radio range. But in a multihop network, nodes depend on intermediate nodes to transmit when the destination node is out of their communication range. MANET has the capacity to create a self-maintaining and self-configuring network without a centralized infrastructure. Because of these unique characteristics, MANET has become more popular in the industry. Since MANET is used widespread, security became an important issue. The majority of routing protocols that have been proposed for MANET assumes that each node in the network is a peer and not a malicious node. Therefore, only a node that compromises with an attacking node can cause the network to fail. Hence an intrusion-detection system (IDS) specially designed for MANETs is to be developed to overcome the security issues.

II. IDS IN MANETs

An intrusion detection system is a security system that detects inappropriate or malicious activity on a computer or network. IDS are used to determine if a computer network has experienced an unauthorized intrusion. Due to the limitations of most of the routing protocols of MANETs, nodes assume that other nodes always cooperate with each other to relay data. This assumption gives opportunities to attackers to attack the network with just one or two compromised nodes. In order to address this problem, IDS should be added to improve the MANETs security level. If MANET can detect the intruders as soon as they enter the network, the potential damages caused by compromised nodes at first time. In this section, we mainly describe three existing approaches, namely, Watchdog [5], TWOACK [14], and Adaptive Acknowledgment (AACK) [15].

A. WATCHDOG

Marti et al. proposed a reputation-based scheme. Two modules called watchdog and pathrater are implemented for each node to detect and mitigate routing misbehaviors in MANETs. Nodes operate in a promiscuous mode by which the watchdog module overhears the medium to check if the next-hop node forwards the packet or not. At the same time, it maintains a buffer of recently sent packets. When the watchdog overhears the same packet being forwarded by the next hop node over the medium, that packet is cleared from the buffer. If a data packet remains in the buffer too long, the watchdog module accuses the next hop neighbor to be misbehaving. Thus, the watchdog enables misbehavior detection while forwarding packets as well as at the link. Based on watchdog's accusations, the pathrater rates every path in its cache and subsequently chooses the path that best avoids misbehaving nodes. However, the watchdog technique may fail to detect misbehavior in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior report, collusion and partial dropping.

1) Ambiguous collisions: As shown in Fig.1, ambiguous collision occurs at A while it is listening for B to forward a packet on. Node A does not know whether the collision is caused by its neighboring nodes or by node B.

2) Receiver collisions: Due to the receiver collision problem node A can only tell whether B sends the packet to C, but it cannot tell whether C received it. Node C might not receive the packet because of a collision.

3) False misbehavior report: For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, node A still reported node B as misbehaving.

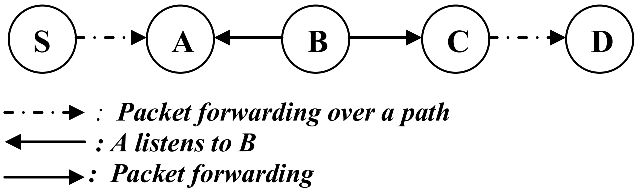


Fig.1. Passive Acknowledgment

4) Limited transmission power: A node can limit its transmission power such that a signal is sufficiently strong to reach the previous node while weak enough not to reach the true recipient.

5) Collusion: Here more than one misbehaving node can collude to disrupt the Watchdog mechanism. For example, B forwards a packet to C but B does not report to A when C drops the packet.

6) Partial dropping: When a node drops packets at a rate lower than the configured misbehaving threshold, partial dropping occurs.

B. TWOACK

To overcome the problems of limited transmission power and receiver collision of Watchdog, Liu et al. [14] proposed a network-layer scheme called TWOACK in order to detect misbehaving nodes. When a node forwards a packet, the node's routing agent checks whether the packet is received successfully by the node that is two hops away on the source route.

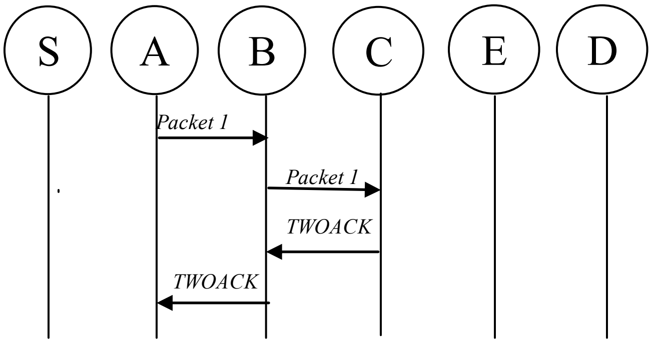


Fig.2. TWOACK scheme

This is done through the use of a special type of acknowledgment packets named TWOACK packets. A node acknowledges the reception of a data packet by sending back a two-hop TWOACK packet along the active source route. If the sender of a data packet does not receive that packet corresponding to a particular data packet that was sent out, the next-hop's forwarding link is detected to be misbehaving and the forwarding route broken. Based on this, the routing protocol avoids the malicious link in all future routes, which results in an improved overall throughput for the network.

The working process of TWOACK is shown in Fig. 2. Node A first forwards Packet 1 to node B, and then, node B forwards the same to node C. When node C receives Packet 1, since its two hops away from node A, node C generates TWOACK packet, which takes reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this packet is not received in the particular time period, both nodes B and C are reported malicious. The same process is carried out in the three consecutive nodes along the rest of the route. However, the acknowledgment process done during packet transmission process adds a significant amount of unwanted network overhead. Due to the limited battery power in MANETs, such transmission process can easily degrade the life span of the entire network.

C. AACK

Sheltami et al. [15] proposed a new scheme called AACK which is based on TWOACK. AACK is an acknowledgment based network layer scheme which can be considered as a combination of TACK (similar to TWOACK) and an end-to-end acknowledgment scheme called Acknowledge (ACK). Compared to TWOACK, AACK reduced network overhead while still capable of maintaining the same network throughput.

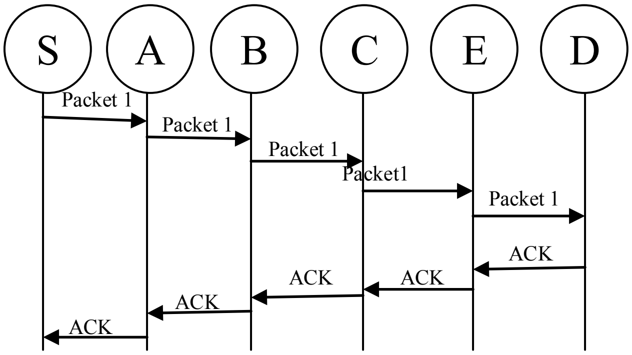


Fig.3. ACK scheme

In the ACK scheme shown in Fig. 2, the source node S sends out Packet and the other upcoming nodes simply forward this packet and when the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a specific time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. This concept of AACK greatly reduces the network overhead, but both TWOACK and AACK fails to detect malicious nodes in the presence of false misbehavior report and forged acknowledgment packets. Hence an acknowledgment based scheme which largely depends on the acknowledgment packets is required. It is also necessary that the acknowledgment packets should be valid and authentic. So we use digital signature concept in the scheme named Enhanced AACK (EAACK).

III. EAACK

In this paper, we propose a special type of Intrusion Detection system named EAACK which is mainly designed to tackle three of the six weaknesses of Watchdog scheme, namely false misbehavior, limited transmission power and receiver collision. Here, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgement packets.

EAACK consists of three major parts namely ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). Here we assume that the link between each node in the network is bidirectional. Then for each communication process, both the source node and the destination node are not malicious and all the acknowledgment packets should digitally signed by the sender and verified by its receiver.

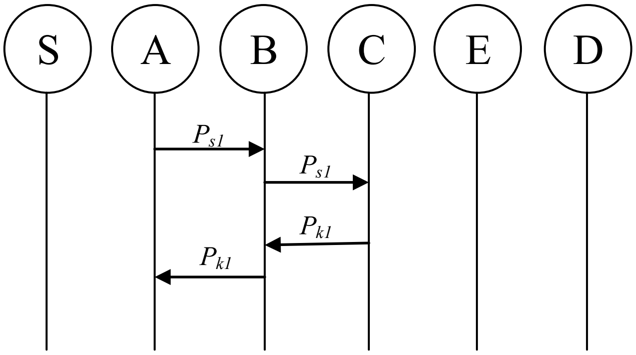


Fig.4. ACK scheme in EAACK

i) ***ACK*****:** ACK is basically an end-to-end acknowledgment scheme and its process is shown in Fig.4 in which node S first sends out an ACK data packet Ps1 to the destination node D. If all the intermediate nodes along the route between nodes S and D co-operate and if node D successfully receives *Ps*1, node D is required to send back an ACK acknowledgment packet *Pk*1 along the same route back. Within a particular time period, if node S receives *Pk*1, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

ii) ***S-ACK:*** The S-ACK scheme is an improved version of the TWOACK. Three consecutive nodes

ISSN: 2278 – 7798

work in a group to detect nodes that are misbehaving. Suppose if three consecutive nodes are present in the route, the third node has to send an S-ACK acknowledgment packet to the first node. The S-ACK mode is introduced to detect misbehaving nodes in the presence of receiver collision or limited transmission power. Moreover, a misbehavior report will be generated and sent to the source node S. EAACK requires the source node to switch to MRA mode and confirm this misbehavior report.

iii) MRA: The MRA scheme is designed to resolve the problem of false misbehavior report during malicious node detection. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

To begin with MRA mode, the source node first searches its database and checks if any alternative route to the destination node is present. If no route exists, the source node starts a DSR routing request to find another route. Since we are using MANETs, it is common to find out multiple routes between two nodes. By choosing an alternative route to the destination node, we avoid the misbehavior reporter node. When an MRA packet is received by the destination node, it searches its database and compares if the reported packet was received. If it is received already, then it is safe to come to conclusion that this is a false misbehavior report and whoever generated this report is reported as malicious. Otherwise, the misbehavior report is trusted and accepted. By this technique of MRA scheme, EAACK detects malicious misbehavior of nodes even during the presence of false misbehavior report.

iv) Digital Signature: EAACK is an acknowledgment-based IDS. All three parts of EAACK are acknowledgment-based detection schemes. As they depend on acknowledgment packets to detect misbehaviors in the network, it should be ensured that all acknowledgment packets in EAACK are authentic; otherwise all of the three schemes will become vulnerable to attacks. Hence we use digital signature in order to ensure integrity of the IDS. In EAACK all acknowledgment packets is to be digitally signed before they are sent out and verified until they are accepted.

IV.SIMULATION AND PERFORMANCE

Simulation results have been taken for Packet Delivery Ratio, Overhead, Throughput and Delay.

A. Simulation Parameters

Channel	Wireless
Network Interface	Wireless
NS Version	NS-2
Simulation time	80s
Number Of Nodes	42
MAC Type	MAC 802.11
Packet Rate	1000k
Traffic Type	CBR
Routing Protocol	DSR
Antenna type	Omni directional Antenna

B. Simulation Window

1) WATCHDOG

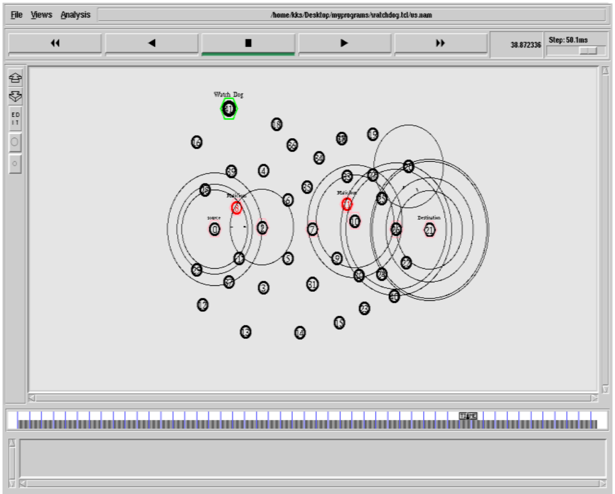
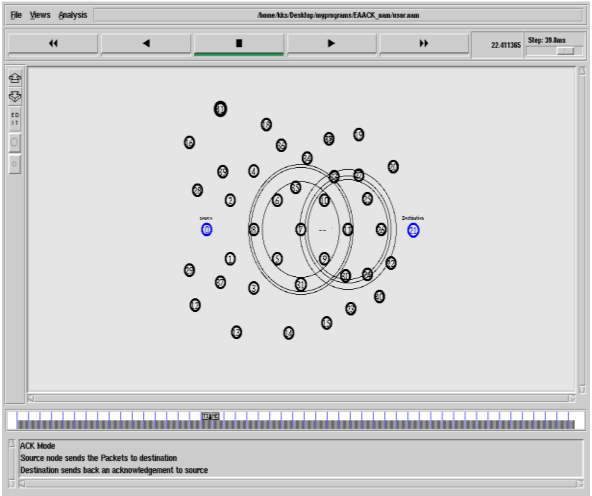


Fig.5. Watchdog scheme

From Fig.5, 42 nodes are taken and packet transmission takes place between them. Watchdog node is represented by the green hexagon. It keeps watching all the nodes and identifies if any malicious nodes are present. The watchdog finds node 8 to be malicious which is represented in red.

The malicious node is replaced by another node 2 and watchdog has detected another malicious node 11.Similarly malicious node 11 is replaced by a node 10. Both the malicious nodes 8 and 11 are replaced by nodes 2 and 10, and the further process is carried out and watchdog keeps watching to find if any other misbehaving nodes are present.

2) *EAACK - ACK scheme*

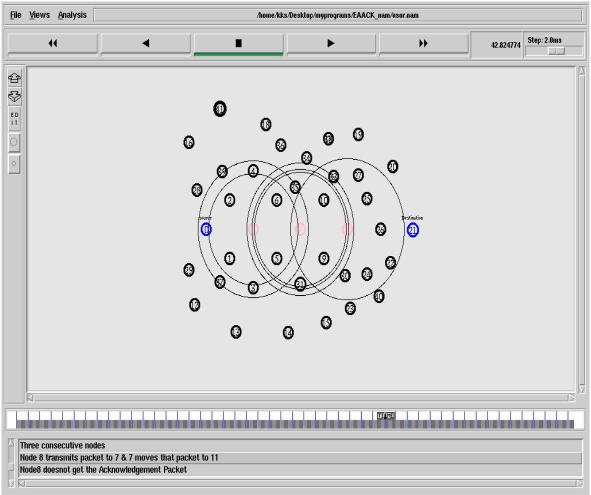


ACK Mode
Source node sends the Packets to destination
Destination sends back an acknowledgement to source

Fig.6. ACK scheme

From Fig.6, Source forwards a packet to destination and the destination sends back an acknowledgement to the source but if acknowledgment is not received within the required time, then it's switched to SACK mode.

3) *EAACK – SACK scheme*

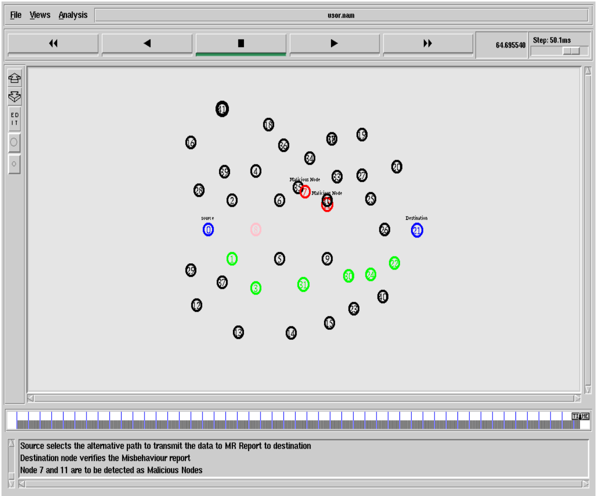


Three consecutive nodes
Node 8 transmits packet to 7 & 7 moves that packet to 11
Node8 doesnot get the Acknowledgement Packet

Fig.7. SACK scheme

From Fig.7, while detecting the misbehaving node, node 8 first forwards packet 1 to node 7, and then node 7 forwards Packet 1 to node 11. Node 11 has to send back an acknowledgment to node 8 that packet has been received. If the packet is not received in a predefined time period, both nodes 7 and 11 are reported malicious.

4) *EAACK-MRA scheme*



Source selects the alternative path to transmit the data to MR Report to destination
Destination node verifies the Misbehaviour report
Node 7 and 11 are to be detected as Malicious Nodes

Fig.8.MRA scheme

From Fig.8, Node 8 transmits the misbehavior report to source node. Source selects an alternative path represented by green color to transmit the MR report to the destination. Destination node verifies the misbehavior report. Node 7 and 11 are detected to be malicious nodes.

C. *Routing Overhead*

Overhead is the ratio of number of routing control packets to delivered data packets achieved. From Fig. 9, a graph for each technique namely Watchdog, TWOACK and EAACK has been plotted and out of these three, EAACK contains less Overhead compared to the other methods.

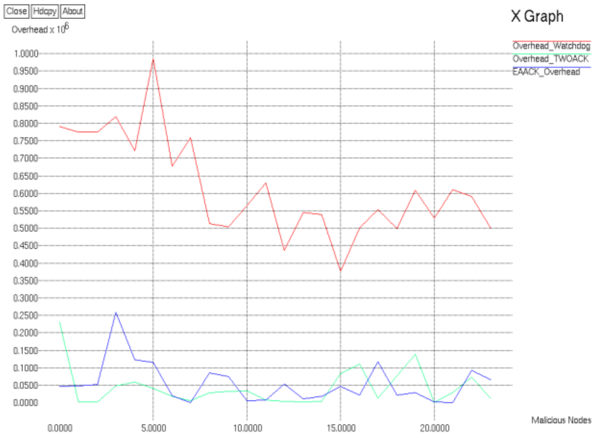


Fig. 9. Overhead versus Malicious Nodes

ISSN: 2278 – 7798

D. *Packet Delivery Ratio (PDR)*

PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

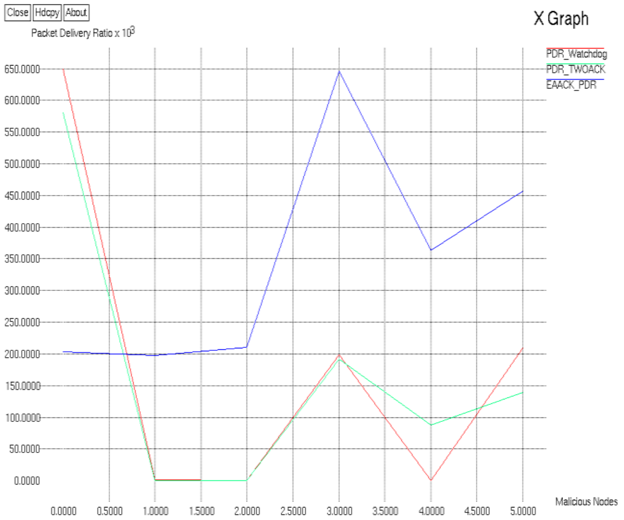


Fig.10. Packet Delivery Ratio versus Malicious Nodes

From Fig.10, a graph for each technique namely Watchdog, TWOACK and EAACK has been plotted and out of these three, EAACK contains more Packet Delivery Ration compared to the other methods.

E. *Throughput*

The term throughput is the ratio of the total amount of data that a receiver receives from a sender to a time it takes for receiver to get the last packet. A low delay in the network translates into higher throughput.

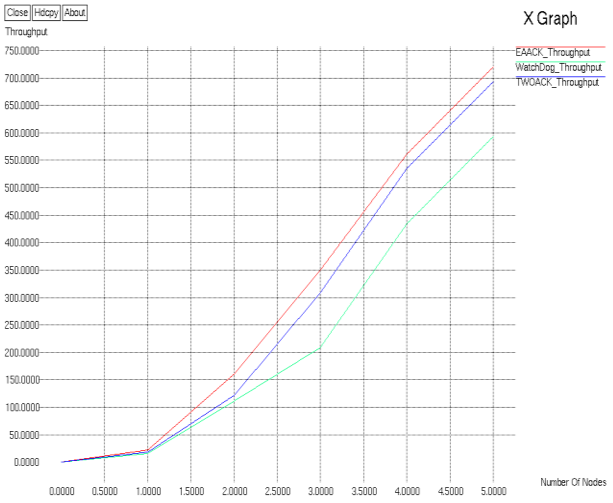


Fig.11. Throughput versus Malicious Nodes

From Fig.11, a comparison graph for the three techniques namely Watchdog, TWOACK and EAACK is drawn out of which Eaack has the largest throughput compared to the other methods.

F. *Delay*

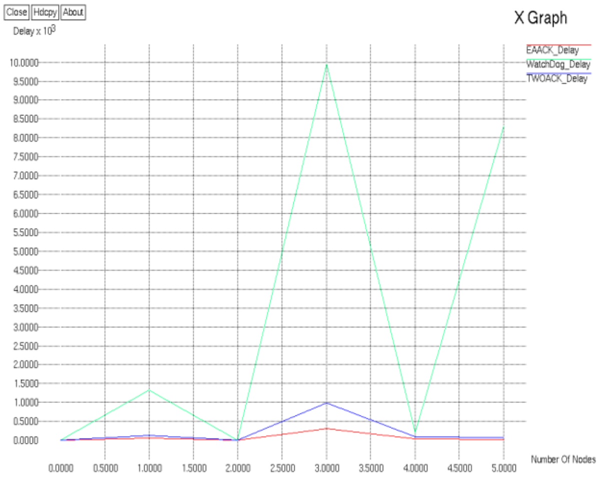


Fig.12. Delay versus Malicious Nodes

The delay of a Network specifies how long it takes for a packet to travel from one node to the other node. Delay may differ slightly, depending on the location of the specific pair of communicating nodes. From Fig.12, a comparison graph for the three techniques namely Watchdog, TWOACK and EAACK is drawn out of which Eaack has the largest lowest delay compared to the other methods.

G. *Comparison Table*

TABLE 1 ROUTING OVERHEAD

IDSs	Malicious Nodes					
	0%	5%	10%	15%	20%	25%
Watchdog	0.78	0.97	0.56	0.39	0.53	0.50
TWOACK	0.23	0.05	0.03	0.07	0.03	0.05
EAACK	0.05	0.25	0.01	0.04	0.01	0.05

TABLE 2 PACKET DELIVERY RATIO

IDSs	Malicious Nodes					
	0%	1%	2%	3%	4%	5%
Watchdog	650	0	0	200	0	210
TWOACK	580	0	0	190	80	140
EAACK	210	200	230	640	360	460

TABLE 3 THROUGHPUT

IDSs	Malicious Nodes					
	0%	1%	2%	3%	4%	5%
Watchdog	0	10	101	210	440	595
TWOACK	0	12	110	305	545	640
EAACK	0	45	170	350	570	730

TABLE 4 DELAY

IDSs	Malicious Nodes					
	0%	1%	2%	3%	4%	5%
Watchdog	0	1.2	0	9.8	0.45	8.4
TWOACK	0	0.12	0	1.0	0.9	0.2
EAACK	0	0	0	0.4	0.1	0.1

VI. CONCLUSION AND FUTURE WORK

An efficient IDS named EAACK specially designed for MANETs is developed and its results are compared against other popular mechanisms in different scenarios through simulations. Routing Overhead, Packet Delivery Ratio, Throughput and Delay has been calculated. The results demonstrated positive performances against Watchdog and TWOACK in the cases of receiver collision, limited transmission power, and false misbehavior report.

Though EAACK is an efficient method, it fails to detect malicious misbehavior of the nodes in the presence of three main problems namely Collusion, Ambiguous collisions and Partial dropping that affects the network to a large extent and fails to improve their performance in MANETs. Hence an enhanced intrusion detection mechanism can be proposed to mitigate the above three problems in MANETs since it is the major problem to be avoided.

VII. REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami (2013), 'EAACK—A Secure Intrusion-Detection System for MANETs', IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, pp.1089-1098.

[2] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan (2007), 'An acknowledgment-based approach for the detection of routing misbehavior in MANETs', IEEE Transactions on Mobile Computing, Vol. 6, No. 5, pp. 536–550.

[3] Y. Hu, D. Johnson, and A. Perrig (2002), 'SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks', Proceedings of 2002 4th IEEE Workshop on Mobile Computing System Applications, pp. 3–13.

[4] Y. Hu, A. Perrig, and D. Johnson (2002) 'ARIADNE: A secure on-demand routing protocol for ad hoc networks', Proceedings of 2002 8th ACM International Conference on. Mobile Communications in Atlanta, GA, pp. 12–23.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker (2000), 'Mitigating routing misbehavior in mobile ad hoc networks', Proceedings of 6th Annual International Conference on Mobile Computing Network, Boston , pp. 255–265.

[6] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi (2004), 'On intrusion detection and response for mobile ad hoc networks', Proceedings of 2004 IEEE International Conference on Computer Communications, pp. 747–752.

[7] Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis (2005), 'Secure routing and intrusion detection in ad hoc networks', Proceedings of 2005 3rd International Conference on Pervasive Computer Communication, pp. 191–199.

[8] B. Sun (2009), 'Intrusion detection in mobile ad hoc networks', Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[9] L. Zhou and Z. Haas (1999), 'Securing ad-hoc networks', IEEE Networking, Vol. 13, No. 6, pp. 24–30.

[10] Zougagh Hicham, Toumanari Ahmed, Latif Rachid and Idboufker Noureddin (2012) 'Evaluating and Comparison of Intrusion in Mobile ad hoc networks', International Journal of Distributed and Parallel Systems, IJDPS Vol.3, No.2, pp.243-259.

[11] S.Tamilarasan and Dr.Aramudan (2011), 'A Performance and Analysis of Misbehaving node in MANET using Intrusion Detection System', International Journal of Computer Science and Network Security, IJCSNS Vol.11 No.5, pp.258-264.

[12] Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balakrishnan (2007),' An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs', IEEE transactions on Mobile Computing, Vol. 6, No. 5, pp. 536-550.

[13] S.Neelavathy Pari D.Sridharan (2011), 'A Performance Comparison and Evaluation of Analyzing Node Misbehavior in MANET using Intrusion Detection System', IJCSET, Vol 1, Issue 1, 35-40.

[14] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[15] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 4, pp. 1835–1841, Apr. 2008.