ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Secure IDS for MANETs Using EAACK

Ganesh Munde

M.E. Student, Dept. of Computer, Dr D.Y.Patil School of Engineering, Savitribai Phule Pune University, Pune, India

ABSTRACT: The wireless network has been hugely adapted and has become a global trend since its evolution. One of the most unique applications among other types of wireless network is MANET MANET (Mobile Ad hoc NETwork). Unlike conventional wireless networks, MANET doesn't depend on a fixed infrastructure which makes it unique. Each node in the MANET is equipped with transceiver functionality. When nodes in the MANET are within communication rage, the directly communicate with each other or else they rely on neighbors for transmitting the packets. MANET doesn’t require a centralized infrastructure and provide the ability of self-configuring to individual nodes and this ability made it famous in mission critical use such as military or emergency however it’s vulnerable to malicious attacks because of open medium and distributed nodes. Hence it becomes very crucial to design and develop intrusion detection system (IDS) to protect it from attacks. We have proposed a new intrusion detection system specially designed for MANETs called EAACK (Enhanced Adaptive ACKnowledgment). EAACK is very efficient and doesn’t greatly affect the overall network performance.

KEYWORDS: Enhanced Adaptive ACKnowledgment (EAACK), Digital Signature, Mobile Ad hoc NETwork (MANET), Intrusion detection system (IDS)

I. Introduction

Wireless network allows data communication between many nodes and maintain their ability to move around. But, this communication is held back by the range of transmitters. Because of this, for two nodes to communicate with each other they must be within the communication range otherwise communication is not possible. In order to solve this problem MANET allows nodes to relay data transmissions.

MANET a collection of mobile devices prepared with a wireless transmitter as well as a receiver that communicate with each other via wireless links either directly or indirectly. It is wireless, self-configuring, infrastructure-less network of multiple mobile nodes. MANET is categorized into two basic types i.e. Single-hop and Multi-hop. The difference between the two being first type allows all nodes to communicate directly and later rely on intermediates to transmit the packets if destination is beyond communication range. Unlike conventional wireless network, has a decentralized network infrastructure which allows all clients to maintain mobility [10].

Minimal configuration, easy and quick deployment makes MANET popular and highly recommendable to be used in emergency circumstances where in infrastructure is not already installed and available or when it is not feasible to install the infrastructure in scenarios such as human-induced or emergencies, natural disaster and military operations.

MANET is becoming very popular in mission critical applications; However, Network security is the major concern that needs to be addressed in MANET. Because of open medium and remote distribution, it is vulnerable to malicious attacks. As there is no physical protection to nodes, attackers can easily compromise the security of nodes. Due to pre-assumption of routing protocols that every node is cooperative and it’s not malicious, the attacker can easily compromise MANETs by introducing non cooperative or malicious nodes into the network. For these reasons, it becomes very crucial to develop an effective IDS specially designed for MANETs [6]–[9], [15].

II. Background

A. *Traditional IDS in MANETs*

Many researches have been carried out and many approaches have been recommended to develop secure IDS for MANET. An IDS acts as a secondary layer in MANET and greatly complements the existing functionalities. Below are some existing IDS which are designed especially for MANETs

1. *WatchDog*

This IDS monitors the activities in MANET to detect the misbehavior or malicious activities. The Watchdog technique basically has two parts, called, Watchdog and Pathrater. When a node forwards any packet, the watchdog module in a node continuously listen to other nodes within the range to check if the next node in the set also forwards the same packet. When a Watchdog node discovers that its neighbour node is failing continuously to forward the packet within a period of time, it increases the failure counter for that particular node. Watchdog scheme reports the node as misbehaving when the failure count of that node exceeds the predefined threshold values for failure counter. Whenever any node is reported as misbehaving, the Pathrater part comes into the picture. The job of Pathrater is to cooperate with the routing protocols and avoid reported node in future transmission. WatchDog scheme is effective and easy to implement which makes it a popular choice in MANET. Many IDS in MANET are either based on Watchdog scheme or developed as an improvement to it [15]. However this approach is unable to detect misbehaviors in case of receiver collisions, ambiguous collisions, limited transmission power, false misbehavior report, collusion, and partial dropping. Watchdog scheme can detect malicious node not malicious link.

2. *TWOACK*

Many researches are done to solve these six weaknesses of watchdog. TWOACK scheme is one of the the most important approaches amongst them. TWOACK is neither enhancement nor a watchdog system unlike other approaches. TWOACK scheme detects misbehaving links by acknowledging every single packet transmitted over every three consecutive nodes along the path from the source to the destination. When packet is received, each node along the route sends back an acknowledgment to a node that is two hops away from it. Fig. 2.1 shows the overall working of TWOACK scheme.

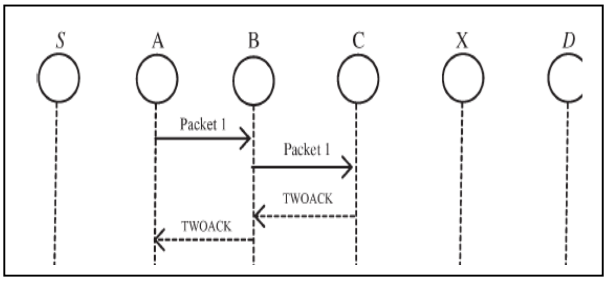


Fig. 2.1 TWOACK scheme: Each node sends back an acknowledgment to the node that is two hops away from it

As shown in fig. 2.1, Node A sends a packet to node B, and node B forwards it to node C. As node C is two hops away from node A, it has to generate a TWOACK packet and send it back to node A via reverse route. When node A receives this TWOACK packet, the transmission from node A to node C is successful. If TWOACK packet is not received by node A in a predefined time period, B and C nodes are reported malicious. The same process is carried out for over every three consecutive nodes along the rest of the route.

TWOACK successfully solves the receiver collision and limited transmission power weaknesses of WatchDog, but redundant transmission degrades the overall performance of the network

3. *AACK*

AACK is based on TWOACK scheme. It is an Adaptive Acknowledgment-based scheme which combines a TWOACK and ACKnowledge(ACK) policies. As compared to TWOACK, AACK has better network throughput and significantly reduces network overhead. The ACK is basically an acknowledgment scheme and it works as shown in Fig. 2.

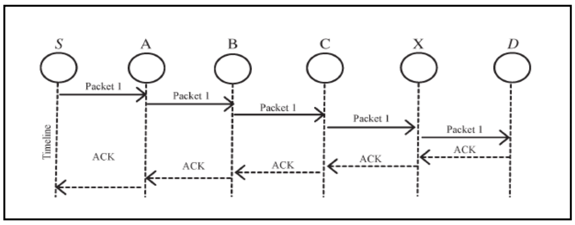


Fig. 2.2 ACK scheme: The destination node sends acknowledgment packet to the source node

AACK scheme is straightforward and works in a simple manner, source node S sends out Packet 1 to Destination node D. All intermediate nodes in route just forward this packet 1. Upon receiving the packet 1, destination node D, sends back an ACK packet to the source node S along the reverse route. The transmission is successful when within a predefined period of time; the source node S receives this ACK packet. If ACK packet is not received by source S, it switches to TWOACK scheme by sending out a TWOACK packet. The combination ACK and TWOACK in AACK scheme greatly reduces the network overhead. However AACK scheme still fails to detect malicious nodes in presence of false forged acknowledgment packets and misbehavior report. Also it is very important to guarantee that the acknowledgment packets are authentic and valid. To overcome these problems, we adopted a digital signature in our proposed scheme called EAACK (Enhanced AACK).

III. DIGITAL SIGNATURE

A digital signature is a technique that binds an entity/ cryptographic value to the digital data. This binding can be independently verified by receiver as well as any third party. Digital signature is widely adopted for ensuring the authentication, integrity, and non-repudiation. Digital signatures are mainly divided into two categories. 1) Digital signature with appendix: Signature verification process requires original message e.g. (DSA). 2) Digital signature with message recovery: Signature verification process requires no other information the signature itself e.g. RSA [23].

The process of communication with digital signature is shown in Fig. 3.1

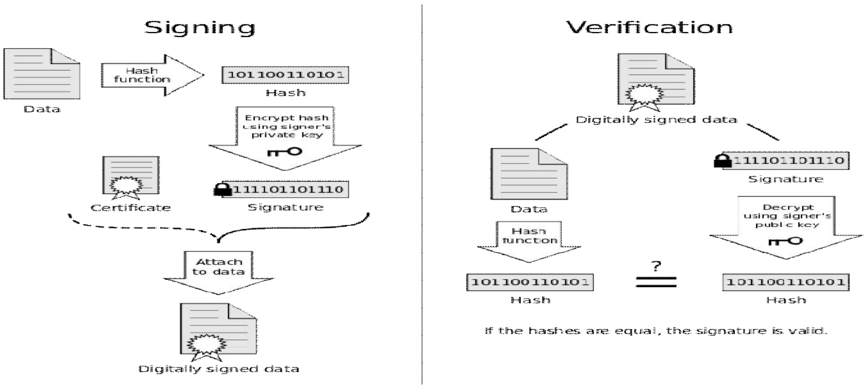


Fig. 3.1 Communication with digital signature

IV. PROBLEM DEFINATION

To develop a secure intrusion detection system for MANET that solves three of the main weaknesses associated with existing scheme i.e. false misbehavior report and forged acknowledgments.

1. *False misbehaviour report*

Node A sends back a misbehaviour report even though node B forwarded the packet to node C.

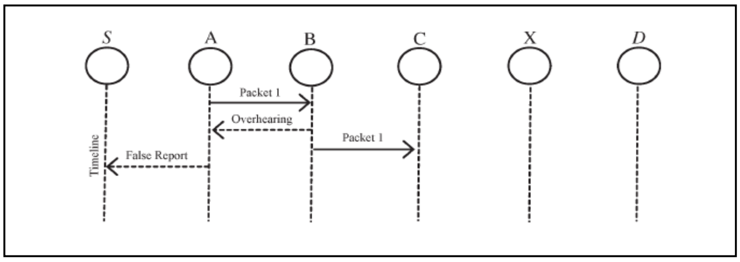


Fig. 4.1 False misbehaviour report

Traditional approaches such as TWOACK and AACK solves the problems of receiver collision and limited transmission power in MANET but they are vulnerable to the false misbehaviour attack. In our approach, our goal is to implement new IDS specially designed for MANETs, false misbehaviour problem and we implement Digital signature to encrypt the all the acknowledgements in the MANET to avoid forging of acknowledgements.

V. Scheme Description

Proposed scheme EAACK consists of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

1. ACK

ACK is end-to-end acknowledgment scheme and works as shown in fig. 5.1. Source node S first sends out an ACK data packet 'Pad1' to the destination D. If all the intermediate nodes along the route are cooperative then destination node D receives 'Pad1'. When node D receives packet 'Pad1' it sends back an ACK acknowledgment packet 'Pak1' along the same route in reverse order. If Source node S receives 'Pak1' within a predefined period of time, then the packet transmission from node S to node D is considered to be successful if not then node S will switch to S-ACK mode by generating S-ACK data packet to detect misbehaving nodes in the same route.

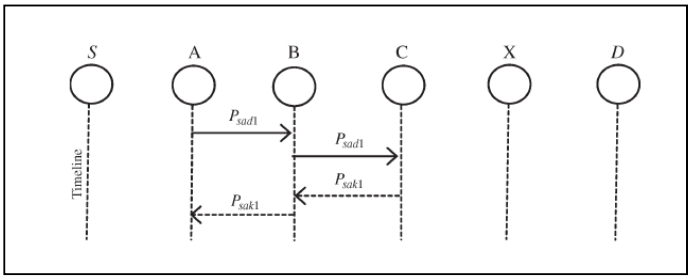


Fig. 5.1 ACK scheme: The destination node sends back an Acknowledgment packet to source node for every packet it receives

2. S-ACK

This scheme is similar to TWOACK scheme. For every three consecutive nodes in the route, the third node is required to send back an S-ACK acknowledgment packet to the first node. The S-ACK scheme is introduced to detect misbehaving nodes in case of a receiver collision or limited transmission power. In S-ACK mode three nodes N1, N2, and N3 work in a group for detecting misbehaving nodes in the network. Node N1 sends out S-ACK data packet 'Psad1' to node N2 and N2 simply forwards it to N3. As soon as N3 receives 'Psad1', it sends back an S-ACK acknowledgment packet 'Psak1' to node N1 via N2 as N3 is the third node in this three-node group. If node N1 doesn't receive 'Psak1' packet within a predefined period of time, N2 and N3 both are reported as malicious. A misbehavior report is generated by node N1 and sent to the source node S.

Unlike TWOACK scheme where the source node immediately trusts the misbehavior report, EAACK does not immediately trust this report. In order to confirm the misbehavior report the source node switches to MRA mode after receiving misbehavior report. This MRA scheme is designed to detect false misbehavior report. Also as we are using digital signatures for acknowledgments, forged acknowledgments are not possible.

3. MRA

Existing IDS in MANET fails to detect misbehaving nodes when false misbehavior report is generated by attacker. To address this limitation, MRA scheme is designed which detect if the false misbehavior report is genuine or generated by attacker.

The MRA scheme authenticates misbehavior report by checking whether the destination node has received the reported missing packet by sending the same packet through a different route.

In MRA mode, the source node find outs an alternative route to the destination node and there is always alternative route to any destination because of structure of MANET. The source node generates MRA Packet and sends it to destination node through a different route. When this MRA Packet is received by destination node, it searches its local knowledge base and checks whether the reported packet was received. If reported packet is already received by destination, then it is safe to conclude that the report was indeed a false misbehavior report and the node that generated this report is marked as malicious. The misbehavior report is trusted if the reported packet was not received earlier, the misbehavior report is trusted and accepted.

The overall working of EAACK System is shown in fig.5.2.

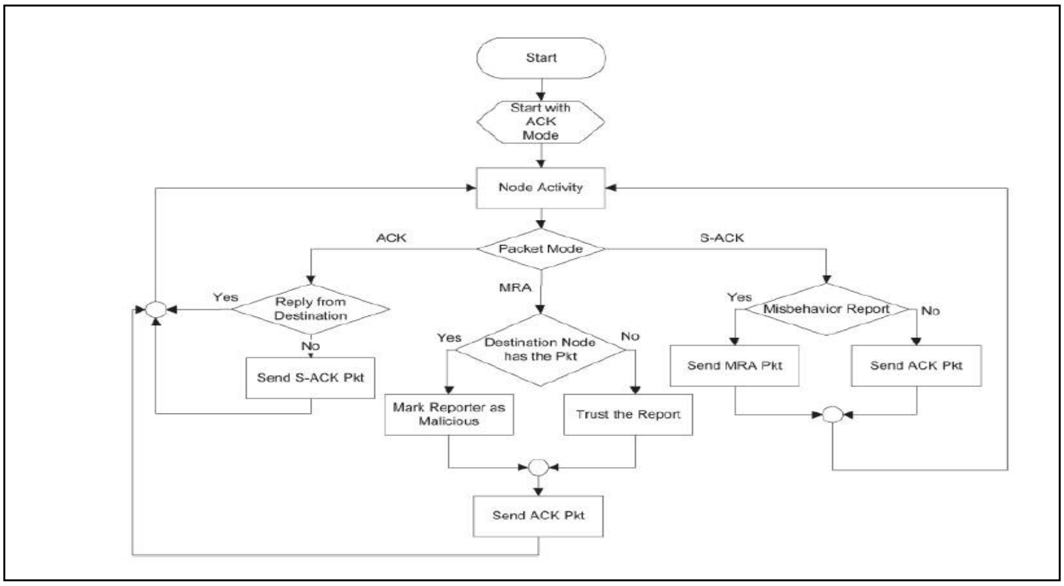


Fig. 4.1.2 System Flow

VI. Simulation Results

In this section, we focus on EAACK performance and results and discuss about simulation environment and methodology for EAACK. We discuss ways of comparing performances through simulation result comparison with Watchdog, TWOACK, and AACK schemes.

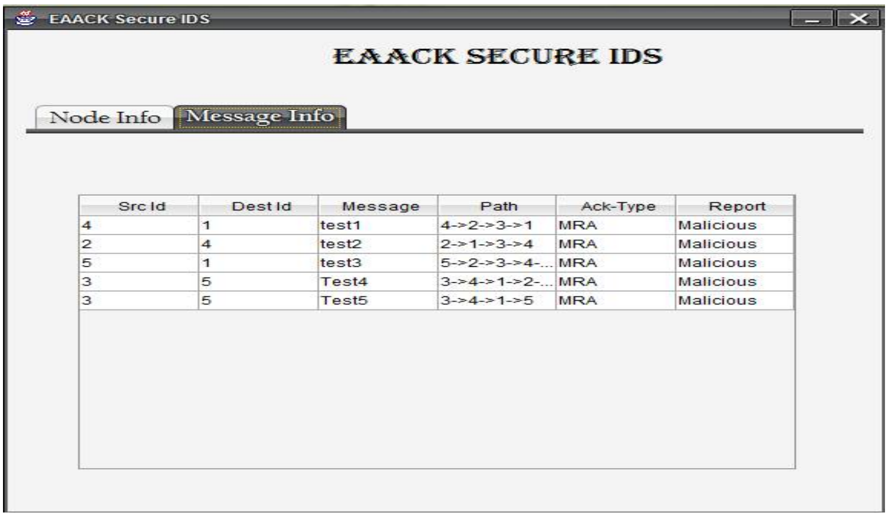
We have used Sun Java Wireless Toolkit 5.2.2 for simulation environment which provides the ability to generate the mobile nodes and help in stimulating the wireless environment.

In order to measure performances of our proposed scheme we adopted PDR (Packet delivery ratio as) as parameter. PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

We proposed three scenario settings to simulate different types of misbehaviors or attacks to better investigate the performance of EAACK under different types of attacks.

Scenario 1: In this scenario, we try to simulate ability to system to detect the malicious nodes when all the nodes are malicious. This is worst case negative scenario where system successfully detects the malicious nodes but its performance is surely less than other systems as its check if the packet is already received or not using MRA model.

Fig. 6.1 shows the system output in this scenario.

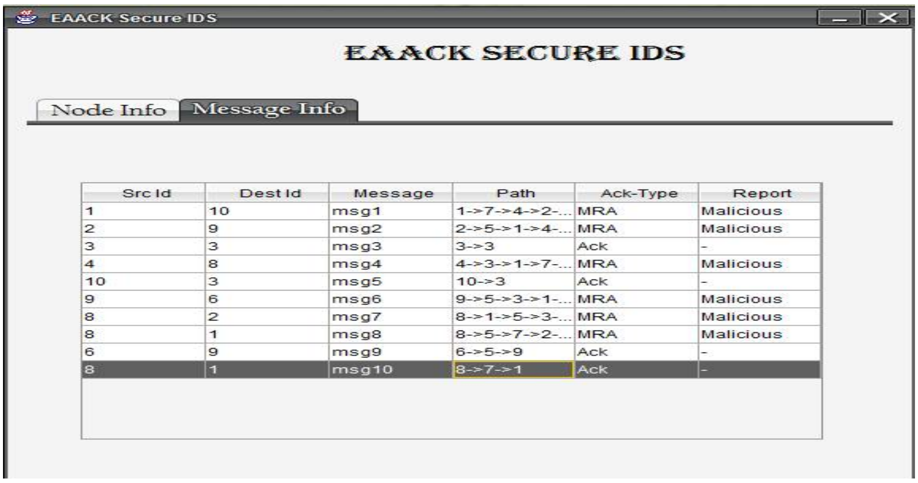


Src Id	Dest Id	Message	Path	Ack-Type	Report
4	1	test1	4->2->3->1	MRA	Malicious
2	4	test2	2->1->3->4	MRA	Malicious
5	1	test3	5->2->3->4-...	MRA	Malicious
3	5	Test4	3->4->1->2-...	MRA	Malicious
3	5	Test5	3->4->1->5	MRA	Malicious

Fig. 6.1 Result of simulation scenario 1

As shown in above fig. When all the nodes in the system send malicious MRA report, system successfully detects it.

Scenario 2: In this scenario, we try to test the system when 60% nodes are malicious and they drop the packets they receive. Whenever the malicious nodes are present, system will take slightly more time than existing systems but surely detects the malicious nodes. Fig. 6.2 shows this scenario.

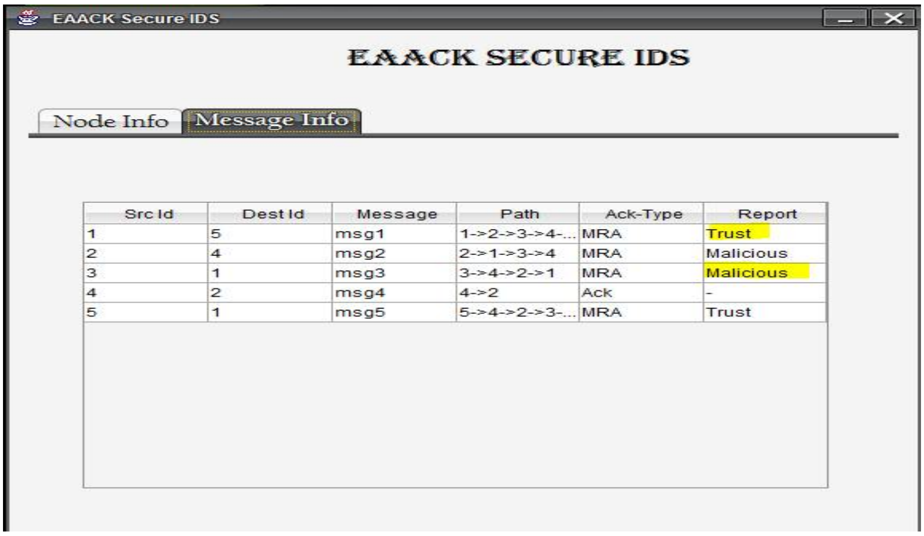


Src Id	Dest Id	Message	Path	Ack-Type	Report
1	10	msg1	1->7->4->2-...	MRA	Malicious
2	9	msg2	2->5->1->4-...	MRA	Malicious
3	3	msg3	3->3	Ack	-
4	8	msg4	4->3->1->7-...	MRA	Malicious
10	3	msg5	10->3	Ack	-
9	6	msg6	9->5->3->1-...	MRA	Malicious
8	2	msg7	8->1->5->3-...	MRA	Malicious
8	1	msg8	8->5->7->2-...	MRA	Malicious
6	9	msg9	6->5->9	Ack	-
8	1	msg10	8->7->1	Ack	-

Fig. 6.2 Result of simulation scenario 2

As shown in above fig, when some of the nodes in the system send malicious MRA and rest of the nodes successfully delivers the message to destination, system detects this behavior.

Scenario 3*:* *T*his scenario designed to detect the malicious nodes in case of false misbehavior report.
Attacker can send false MRA Report even though it receives the packet. EAACK successfully decides if the report is malicious or is to be trusted. Fig 6.3 shows this scenario.

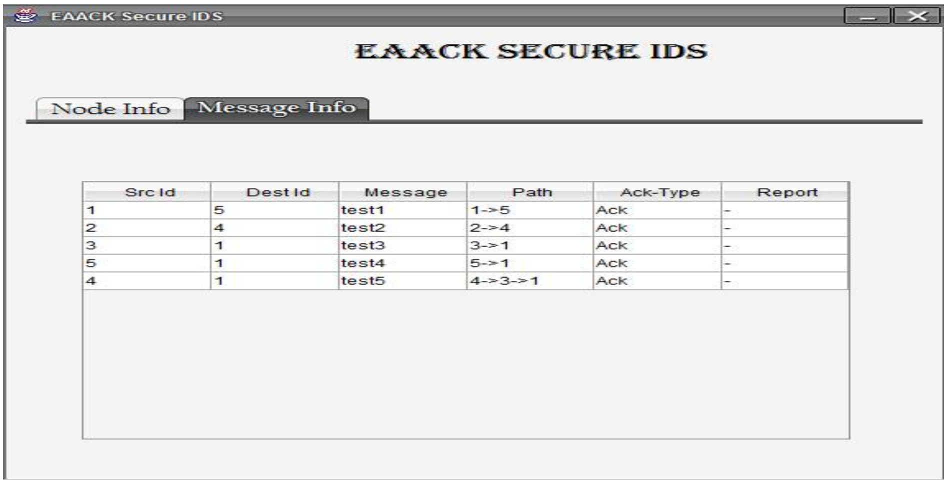


Src Id	Dest Id	Message	Path	Ack-Type	Report
1	5	msg1	1->2->3->4-...	MRA	Trust
2	4	msg2	2->1->3->4	MRA	Malicious
3	1	msg3	3->4->2->1	MRA	Malicious
4	2	msg4	4->2	Ack	-
5	1	msg5	5->4->2->3-...	MRA	Trust

Fig. 6.3 Result of simulation scenario 3

As shown in above fig. When few nodes in the system drops the packet and but they are not malicious, system successfully detects this behaviour by sending the packet through different route.

Scenario 4*:* This scenario happy path scenario when no node is malicious in the system. The performance is improved in this case there is no need to check if the destination has received the message. It is shown in Fig.6.4



Src Id	Dest Id	Message	Path	Ack-Type	Report
1	5	test1	1->5	Ack	-
2	4	test2	2->4	Ack	-
3	1	test3	3->1	Ack	-
5	1	test4	5->1	Ack	-
4	1	test5	4->3->1	Ack	-

Fig. 6.4 Result of simulation scenario 4

As shown in fig. When there is no malicious node in the system, it works efficiently.

VII. CONCLUSION AND FUTURE SCOPE

We have proposed secure IDS named EAACK specially designed for MANETs. We checked the performance of our system through simulation in presence of False Misbehavior report. The results we found are positive against when there are malicious nodes in the system and in presence of false misbehavior reports. In future, we will try to investigate and implement the following issues in our research:

1) We will try to examine the possibilities of adopting hybrid cryptography techniques to avoid digital signature as it can cause network overhead.

2) We will try to examine the possibilities of adopting different key exchange mechanisms to eliminate the requirement of pre distributed keys.

3) We would like to test the performance of EAACK in real network environment instead of simulation environment.

REFERENCES

1. N. Soms, R. Saji Priya, A.S. Banu, P.Malathi," A Comprehensive Performance Analysis of Zone Based Intrusion Detection System in Mobile Ad Hoc Networks", IEEE Publisher, pp.1-8,26-28, March 2015..
2. S.Adhikari and S.K. Setua," Cooperative Network Intrusion Detection System (CNIDS) in Mobile Adhoc Network Based on DSR Protocol", IEEE Publisher, pp. 929 - 935, 12-13, Oct.2013.
3. R. H. Akbani, S. Patel, and D. C. Jinwala,"DoS Attacks in Mobile Ad Hoc Networks: A Survey", in Proc. 2nd International Meeting ACCT, pp. 535541, 2012.
4. A. Singh, M. Maheshwari, and N. Kumar, "Security and Trust Management in MANET", Communications in Computer and Information Science, New York: Springer-Verlag, vol. 147, pt. 3, pp. 384387, 2011.
5. N. Kang, E. Shakshuki, and T. Sheltami,"Detecting Misbehaving Nodes in MANETs", 12th International Conference, Paris, France, pp. 216222, Nov. 810, 2010.
6. J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros-Mendez,"Energy Harvesting from Piezoelectric Materials fully Integrated in Footwear", IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 813819, Mar. 2010.
7. A. Tabesh and L. G. Frechette,"A Low-Power Stand-Alone Adaptive Circuit for Harvesting Energy from a Piezoelectric Micropower Generator", IEEE Transaction, vol. 57, no. 3, pp. 840849, Mar. 2010.
8. T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud," Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs", International Journal Multimedia Systems, vol. 15, no. 5, pp. 273282, Oct. 2009.
9. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan,"An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transaction Mobile Computer, vol. 6, no. 5, pp. 536550, May 2007.
10. N. Nasser and Y. Chen,"Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad Hoc Network", IEEE International Conference, pp. 11541159, Glasgow, Scotland, Jun 2007.
11. A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis," Secure Routing and Intrusion Detection in Ad Hoc Networks", 3rd International Conference Pervasive Computer Communication, pp. 191199, 2005.
12. B. Sun,"Intrusion Detection in Mobile Ad Hoc Networks", Ph.D. dissertation, Texas A and M Univ., College Station, TX, 2004.
13. A. Patcha and A. Mishra, "Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks", Radio Wireless ConfERENCE, pp. 7578, 2003. Y. Hu, D. Johnson, and A. Perrig,"SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", 4th IEEE Workshop Mobile Computer System Application, pp. 313, 2002.
14. M. Zapata and Asokan, "Securing Ad Hoc Routing Protocols", ACM Workshop Wireless Secure, pp. 110, 2002.
15. Y. Hu, A. Perrig, and D. Johnson,"ARIADNE: A Secure On- Demand Routing Protocol for Ad Hoc Networks", 8th ACM International Conference MobiCom, Atlanta, GA, pp. 1223, 2002.
16. S. Marti, T. J. Giuli, K. Lai, and M. Baker,"Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", 6th Annual International Conference Mobile Computer Network, Boston, MA, pp. 255265, 2000.
17. R. Rivest, A.Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communication ACM, vol. 21, no. 2,pp. 120126, Feb. 1983.