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. 3, Issue 4, April 2015

Implementation of Enhanced & Adaptive Intrusion Detection System for MANET

Trupti G. Ghongade, Avinash P. Wadhe

ME Second Year, Department of CSE, G.H. Raisoni College of Engg and Management, Amravati (MS), India

Assistant Professor, Dept. of CSE, G.H. Raisoni College of Engg and Management, Amravati (MS), India

ABSTRACT: Mobile Ad hoc network has become one of the most important wireless communication mechanisms. Mobile Ad-hoc Networks (MANETS) is a collection of wireless mobile nodes without any infrastructure support, in which every single node works as both transmitter and receiver .Nodes in MANET can communicates directly with each other when they are in a same communication range. The self-configuring ability of mobile nodes in a MANET made them popular in vital mission applications like military use or emergency recovery. However the open medium of MANET allows them vulnerable to attacks. Because of MANET's distributed architecture and changing topology a traditional centralized monitoring system is not longer feasible in MANET .In this case intrusion detection should be focused as another part before an attacker can damage the structure of the system. So, this work presents various intrusion detection system named as TWOACK, AACK, ACK and Enhanced Adaptive Acknowledgement (EAACK).Enhanced intrusion detection system use digital signature technique to digitally signed packets before they are transmitted to ensure integrity and confidentiality of packets.

KEYWORDS: Mobile Ad hoc Network (MANET), Digital Signature, Enhanced Adaptive Acknowledgement (EAACK),IDS.

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a type of Wireless ad hoc network. Among all the contemporary wireless Networks MANET is one of the most important and unique application. It is deployed in applications like research and rescue, military and disaster recovery.

A Mobile Ad hoc Network is a collection of wireless mobile nodes that are able to communicate with every other nodes without any fixed infrastructure. They can communicate with each other via bidirectional wireless links either directly or indirectly and communication is occurs within the transmission range due to limited resource of energy for each node. This means that two nodes cannot communicate with each other if they are beyond the communication range of they are beyond the communication range of their own. In MANET pair of mobile nodes exchange their message either over a direct wireless links or over a sequence of wireless links including one or more intermediate mobile nodes.

MANET is also capable of creating self- configuring and self-maintaining architecture without the need of any centralized infrastructure, often feasible in critical applications like military conflict, emergency services. These characteristics of MANET make them ready to be used in emergency circumstances where such centralized infrastructure is unavailable. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintaining mobility.

However considering the fact that MANETS are very popular in critical mission applications and because of open medium and wide distribution of mobile nodes make it vulnerable to various types of attacks, at all layers, including in particular the network layer, because the design of most MANET routing protocols assumes that there is no malicious intruder node in the network . So, network security plays an very important role in MANET .Due to nodes lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. Considering the fact that most routing protocols in MANET assume that every node in the network work cooperatively with other nodes, this assumption leaves the attackers with the opportunities to achieve significant on the network with just one or two compromised nodes. To address this drawback, IDS should be added to enhance the security level of MANET.

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. 3, Issue 4, April 2015

II. RELATED WORK

Research and development of intrusion detection has been under way for nearly 29 years. The work is most often cited is technical paper by the Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami [1]. Many Intrusion detection techniques like Credit- based scheme, Reputation –based scheme, Acknowledgement scheme have been proposed to prevent selfishness in MANET. Few researchers Kejun Liu, Jing Deng [11] and Sergio Marti [17] have applied above mentioned techniques for the detection of malicious activities. Providing security by detecting misbehaving nodes in network is an important research goal in MANET. The field is very important for research point of view.

S. Marti, T. J. Giuli, K. Lai, and M. Baker [17] were introduced two techniques, namely, watchdog and pathrater, to detect and mitigate the effects of the routing misbehaviour, respectively. The watchdog technique identifies the misbehaving nodes by overhearing on the wireless medium. The pathrater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. The watchdog technique is based on passive overhearing. Unfortunately, it can only determine whether or not the next-hop node sends out the data packet. The reception status of the next-hop link's receiver is usually unknown to the observer. In order to mitigate the adverse effects of routing misbehaviour, the misbehaving nodes need to be detected so that these nodes can be avoided by all well-behaved nodes. Watchdog technique has advantages and weaknesses. DSR with the Watchdog has the advantage that it can detect misbehaviour at the forwarding level and not just the link level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehaviour, 5) collusion, and 6) partial dropping.

Researchers N. Nasser and Y. Chen [12] introduced a new intrusion detection system called ExWatchdog system to overcome the weakness of watchdog system. ExWatchdog is an improvement of traditional Watchdog system and its function is also of detecting intrusion from malicious nodes and reports that information to the response system, Routeguard. It aims to identify nodes that falsely report other nodes s misbehaving nodes. ExWatchdog system contains two parts: Watchdog and routeguard. Either in watchdog or routeguard, each node updates rating of nodes as it knows according to the information provided by any node in the network. A malicious node could partition the network by claiming that some nodes following it in the path are misbehaving nodes. ExWatchdog detection system is proposed to solve this problem.

In MANETs, routing misbehaviour can severely degrade the performance at the routing layer. Specifically, nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. To detect and mitigate such misbehaviour,2ACK scheme is proposed by Kejun Liu, Jing Den, P K Varshney and Balakrishnan[11].The Watchdog detection system has a very low overhead. Unfortunately, watchdog technique suffers from several problems as described in [17]. The main issue is that the event of successful packet reception can only be accurately determined at the receiver of the next-hop link, but the watchdog technique only monitors the transmission from the sender of the next-hop link. Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, [11] focus on the problem of detecting misbehaving links instead of misbehaving nodes.

2ACK scheme serves as an add-on technique for routing schemes to detect routing misbehaviour and to mitigate their adverse effect. It is used to detect some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. 2ACK scheme send two hop acknowledgment packets in the opposite direction of the routing path. It is a network-layer technique to detect misbehaving links rather than nodes and to mitigate their effects.

N. Kang, E. Shakshuki, and T. Sheltami [6] describes that an ad hoc networks employ a decentralized unstructured networking model that relies on node cooperation for key network functionalities such as routing and medium access. This paper develop a model based on the Sequential Probability Ratio Test to characterize how nodes can differentiate between routes that include misbehaving nodes and routes that do not. An advantage of the model is that the number of observations required to evaluate a route need not be determined in advance, which suits well the dynamic nature of ad hoc networks. It then outline a centralized and a localized approach to detect misbehaving nodes on infected routes identified by the model. This evaluation shows that the localized approach is not only the better

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. 3, Issue 4, April 2015

architectural choice for ad hoc networks but also results in a more accurate exposure of misbehaving nodes while incurring low false positives and low false negatives.

N.Kang, E. Shakshuki, and T. Sheltami [5] also describes that MANET suffers from the threat that it fails to detect misbehaving node when the attackers are smart enough to forge the acknowledgement packets transmitted during communication. This paper introduces an intrusion detection scheme with digital signature algorithm to provide secure transmission against false misbehaviour report and partial dropping. This intrusion detection system assumes that communication link between nodes in the network is bidirectional. Misbehaving nodes also lies in the network, behaving selfishly to preserve their own battery. It assumes misbehaving nodes are intermediate nodes, they are neither the source node nor the destination node. In routing stage they cooperate with other nodes but they drop the packets instead of forwarding to next node. After dropping the packets the misbehaving node generate a forge acknowledgement and sent it to source node in order to conceive the source node. Y. Hu, A. Perrig, and D. Johnson [16] describes that an MANET is a group of wireless mobile nodes, in which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting, assuming trusted environment. This paper present attacks against routing in ad hoc networks, and present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives.

R. Akbani, T. Korkmaz, and G. V. S. Raju [3] discuss security issues and their current solutions in the mobile ad hoc network. Owing to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. This paper first analyzes the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. Then it discusses the security criteria of the mobile ad hoc network and presents the main attack types that exist in it.

Each node in a MANET is capable of acting as a router. Routing is one of the aspects having various security concerns.

R. H. Akbani, S. Patel, and D. C. Jinwala [4] surveyed some common Denial-of-Service (DoS) attacks on network layer namely Wormhole attack, Blackhole attack and Grayhole attack which are serious threats for MANETs and also discuss some proposed solutions to detect and prevent these attacks. Adnan Nadeem, Michael P. Howarth[2] also present a survey of network layer attacks, a critical review of their protection mechanisms and their classification as point detection algorithms or intrusion detection systems.

III. PROPOSED SYSTEM

Proposed system consist four major modules namely,

A. ACK implementation
B. Secure Acknowledgment (S-ACK)
C. Misbehavior Report Authentication (MRA)
D. Digital Signature Validation

A. ACK implementation:

ACK is basically an end – to – end acknowledgment scheme .It is a part of EAACK scheme aiming to reduce the network overhead when no network misbehaviour is detected. In ACK mode, node S first sends out an ACK data packet Pad1 to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order. Within a predefined time period, if node S receives Pak1, 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.

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. 3, Issue 4, April 2015

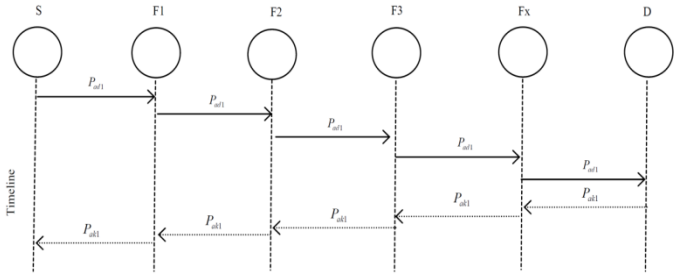

Fig 1.ACK Scheme

B. Secure Acknowledgment (S-ACK):

S-ACK scheme is an improved version of TWOACK scheme [11].The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. In S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet Psad1 to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives Psad1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet Psak1 to node F2. Node F2 forwards Psak1 back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehaviour report will be generated by node F1 and sent to the source node S. Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehaviour report, proposed scheme requires the source node to switch to MRA mode and confirm this misbehaviour report. This is a vital step to detect false misbehaviour report in proposed scheme.

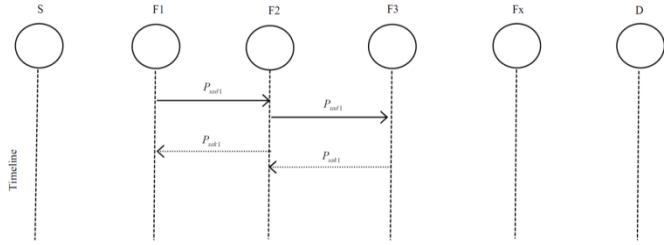

Fig 2.SACK Scheme

C. Misbehaviour Report Authentication (MRA):

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. The false misbehaviour report can be generated by malicious attackers to falsely report innocent nodes as malicious. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, we circumvent the misbehaviour reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted. By the adoption of MRA scheme, proposed system is capable of detecting malicious nodes despite the existence of false misbehaviour report.

D. Digital Signature Validation:

In all the three parts of proposed scheme, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviours in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and unattended. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. In order to

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. 3, Issue 4, April 2015

ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.

IV. SIMULATION

A. Methodology

To better investigate the performance of EAACK under different types of attacks, three scenario settings are proposed to simulate different types of misbehaviours or attacks.

- Scenario 1*:* The purpose of this scenario is to test the performance of proposed IDSs against existing intrusion detection system.
- Scenario 2*:* This scenario, simulate a basic packet dropping attack. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario is to test the performance of IDSs against two weaknesses of Watchdog, namely, receiver collision and limited transmission power.
- Scenario 3*:* This scenario is designed to test IDSs' performances against false misbehaviour report. In this case, malicious nodes always drop the packets that they receive and send back a false misbehaviour report whenever it is possible.

TABLE I

Scenario 1: Ro2uting Overhead

	Number of Nodes:0	Number of Nodes:200	Number of Nodes:400	Number of Nodes :600
TWOACK	0	0.13	0.13	0.13
AACK	0	0.07	0.07	0.08
EAACK(DSA)	0	1.89	1.9	1.9
EAACK(RSA)	0	1.91	1.92	1.92

Scenario 2: Routing Overhead

	Number of Nodes:0	Number of Nodes:200	Number of Nodes:400	Number of Nodes:600
TWOACK	0	122	124	130
AACK	0	72	74	80
EAACK(DSA)	0	180	182	182
EAACK(RSA)	0	200	202	210

Scenario 1: Packet loss Ratio

	Malicious Nodes:0%	Malicious Nodes:10%	Malicious Nodes:20 %	Malicious Nodes :30%
TWOACK	0.1	0.6	0.6	0.73
AACK	0.1	0.75	0.7	0.75
EAACK(DSA)	0	0.01	0.03	0.1
EAACK(RSA)	0	0.06	0.02	0.91

Scenario 2: Packet loss Ratio

	Malicious Nodes:0%	Malicious Nodes:10%	Malicious Nodes:20 %	Malicious Nodes :30%
TWOACK	0	600	700	750
AACK	0	600	600	720
EAACK(DSA)	0	9	8	8
EAACK(RSA)	0	10	9	9

Scenario 1: End-End Delay

	Number of Nodes:0	Number of Nodes:100	Number of Nodes:200	Number of Nodes :300
TWOACK	1	6.5	6.5	6.5
AACK	1	6.3	6.3	6.3
EAACK(DSA)	-1	9	9	9
EAACK(RSA)	0	10	10	10

Scenario 2: End-End Delay

	Number of Nodes:0	Number of Nodes:100	Number of Nodes:200	Number of Nodes:300
TWOACK	1	6.1	6.1	6.1
AACK	1	6.5	6.5	6.5
EAACK(DSA)	10	19	19	19
EAACK(RSA)	6.5	15	15	15

Scenario 3: Routing Overhead

	Number of Nodes: 0	Number of Nodes:200	Number of Nodes:400	Number of Nodes:600
TWOACK	0	125	128	130
AACK	0	74	76	80
EAACK(DSA)	0	175	180	172
EAACK(RSA)	0	210	201	210

Scenario 3: Packet loss Ratio

	Malicious Nodes:0%	Malicious Nodes:10%	Malicious Nodes:20 %	Malicious Nodes :30%
TWOACK	100	600	600	725
AACK	200	890	700	750
EAACK(DSA)	0.1	6	8	8
EAACK(RSA)	0.1	60	12	12

Scenario 3: End-End Delay

	Number of Nodes:0	Number of Nodes:100	Number of Nodes:200	Number of Nodes:300
TWOACK	1	6.4	6.4	6.4
AACK	1	6.2	6.2	6.2
EAACK(DSA)	12	21	21	21
EAACK(RSA)	7.2	16	16	16

B. Simulation Environment

Based on the simulation parameters defined, the mobile ad hoc network is designed as in fig.3 The EAACK is implemented in this environment and its performance is analysed. From figure 4 there are 18 nodes, of which the source node is node 1 and the destination node is node 9. The data is being transferred from source 1 to destination 9

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. 3, Issue 4, April 2015

via the route 1-4-11-9. Based on the behaviour of algorithm, graphs are generated for the performance metrics routing overhead, delay, packet loss ratio.

In the below figure 4 source node is 8 and destination node is 16. The data is being transferred from source 8 to destination 16 via the route 8-4-2-16. Above Fig 6 shows that source node sends data to the destination node in presence of hackers or malicious nodes. When source node does not get acknowledgment from destination node that means after finding malicious node, source node send SACK to the destination node

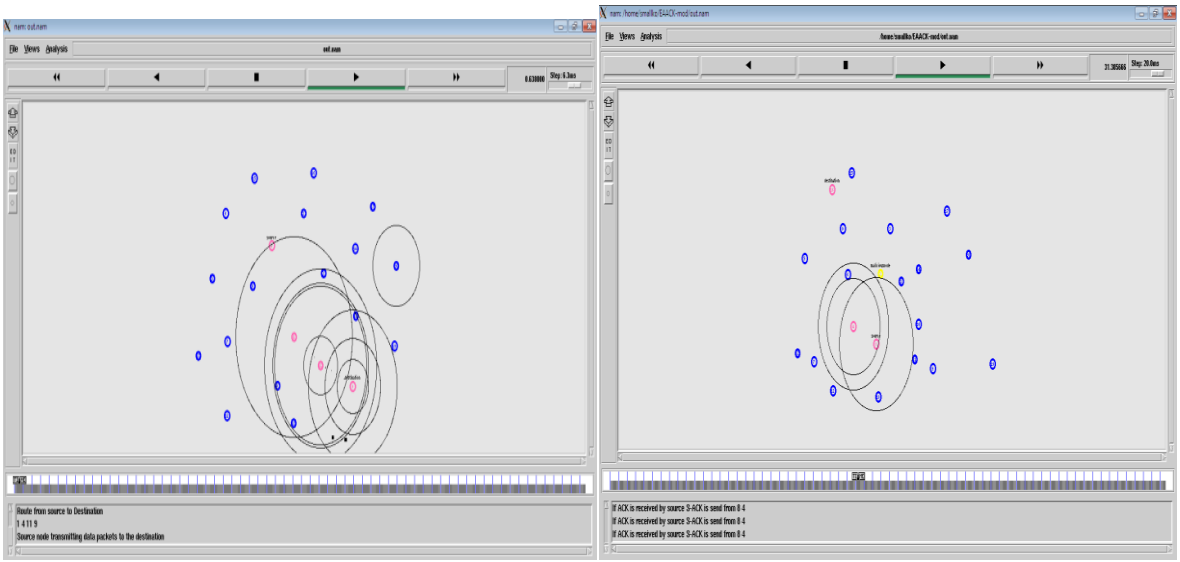

Fig. 3 Simulation Environment

Fig 4 Data transmitted in presence of malicious node

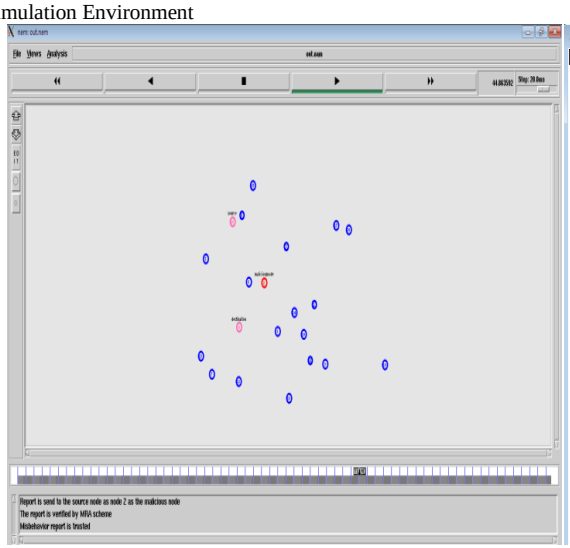

Fig 5 False Misbehaviour report generation

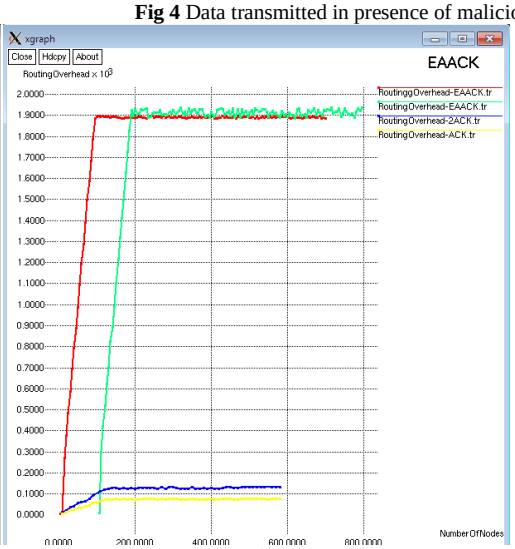

Fig 6. Simulation Result for Scenario 1-Routing Overhead

In figure 5 is the source node and 4 is destination .In this figure false misbehaviour report is generated as node 2 is malicious node and report is send to the source node. After verifying MRA scheme misbehaviour report is trusted and accepted.

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. 3, Issue 4, April 2015

V. PERFORMANCE EVALUATION

A. Simulation Results –Scenario 1:

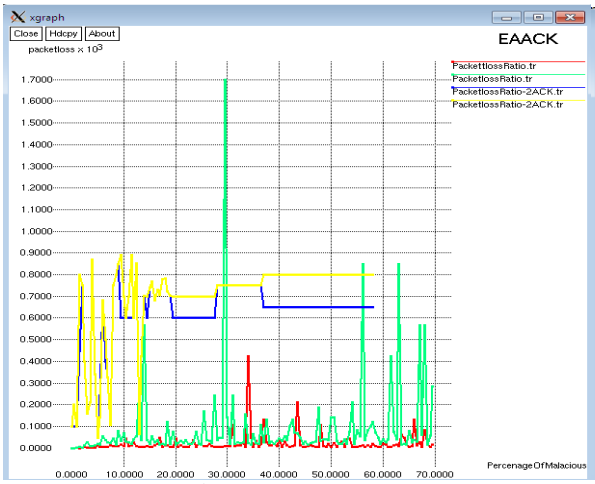

Fig 7. Simulation Result for Scenario 1-PacketLossRatio

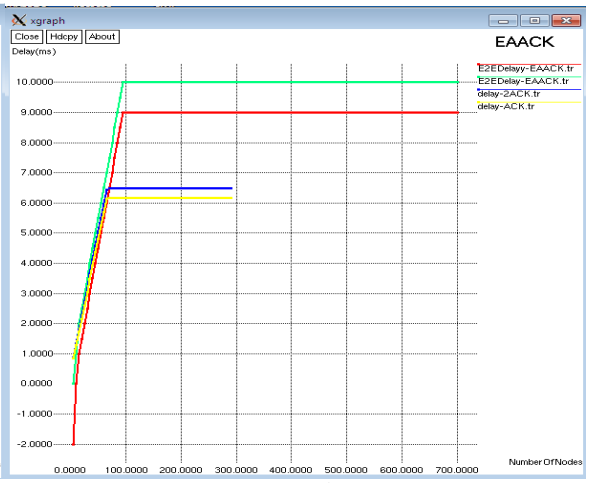

Fig 8.Simulation Result for Scenario 1-End to End Delay

Figure 6. shows the achieved RO performance results for each IDS in scenario 1. Regardless of different digital signature schemes adopted in EAACK, it produces more network overhead than AACK and TWOACK when number of nodes increased. It is conclude that the reason is that digital signature scheme brings in more overhead than the other two schemes.

Results of packet loss ratio are shown in Figure 7.From these results it is conclude that proposed system has greater performance than existing TWOACK, AACK scheme.

B. Simulation Results –Scenario 2:

The results of routing overhead in scenario 2 are shown in below figure 9. AACK acknowledgment has the lowest overhead. This is largely due to its hybrid architecture, which significantly reduces network overhead. Although EAACK requires digital signature at all acknowledgment process, EAACK has more routing overhead. Introduction of DSA in proposed scheme always produces less network overhead than RSA. Because signature size of DSA is much smaller than signature size of RSA. The RO difference between RSA and DSA schemes vary with different number of malicious nodes. The more malicious nodes there are, the more ROs the RSA scheme produced.

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. 3, Issue 4, April 2015

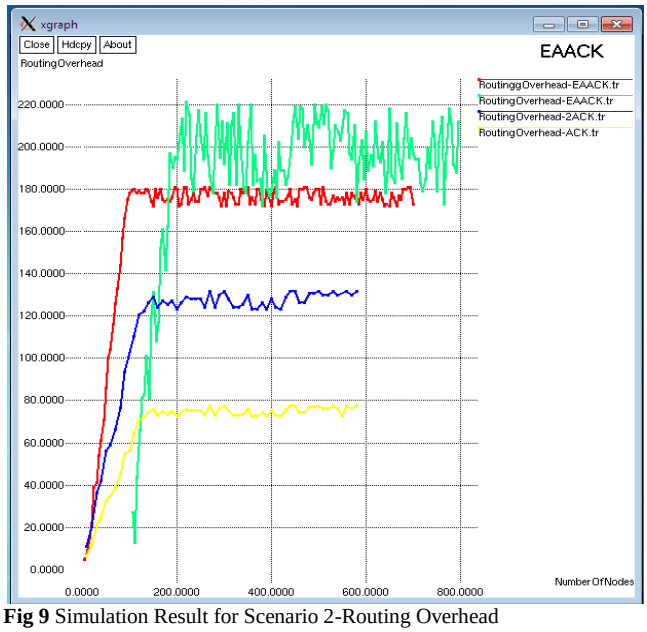

Fig 9 Simulation Result for Scenario 2-Routing Overhead

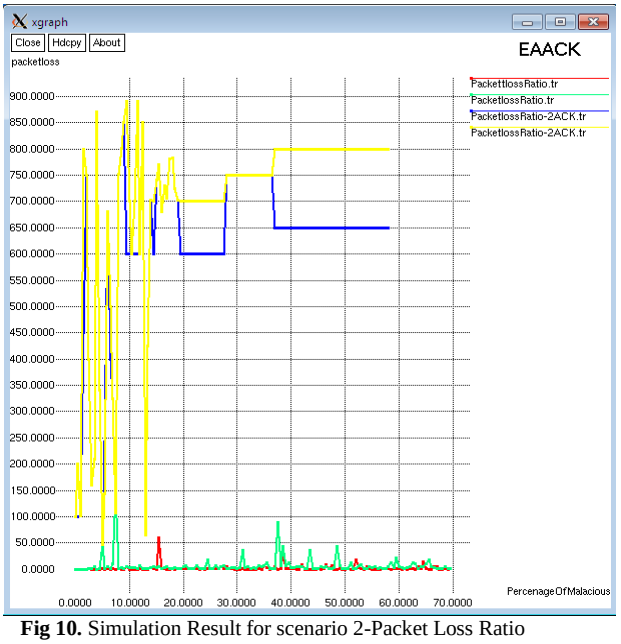

Fig 10. Simulation Result for scenario 2-Packet Loss Ratio

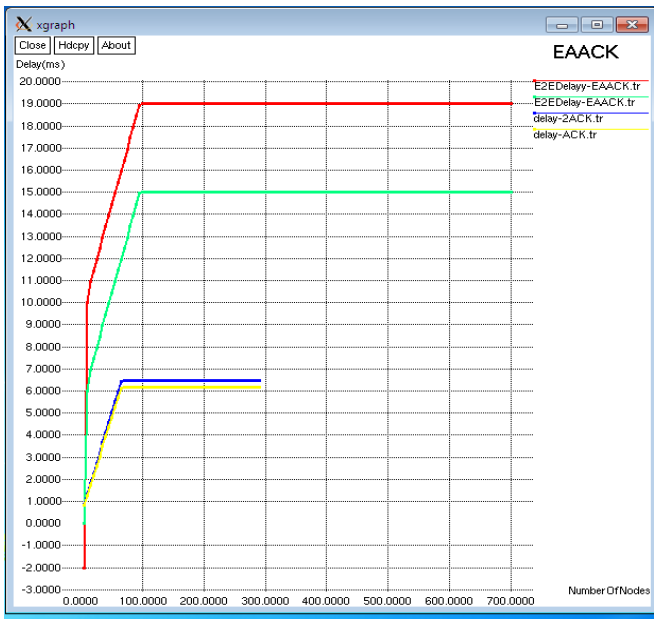

Fig 11. Simulation Results for Scenario 2- End –to-End Delay

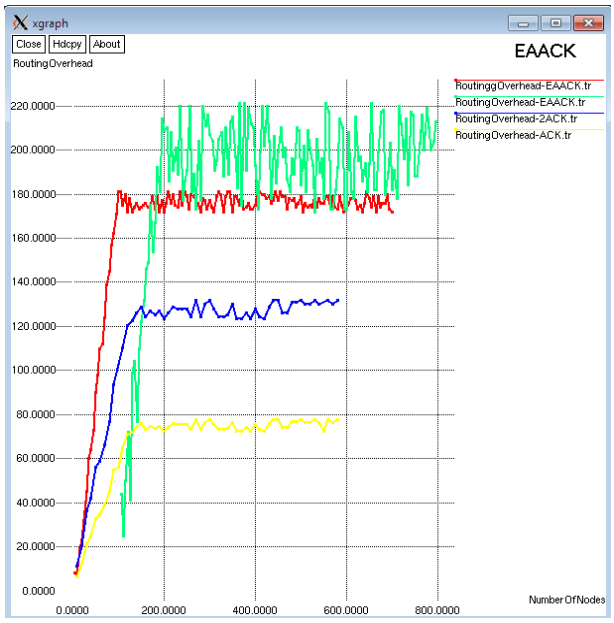

Fig 12 Simulation Results for Scenario 3-Routing Overhead

In scenario 2, malicious nodes drop all the packets that passed through it .Figure 10 shows the simulation results that are based on packet loss ratio. In Fig it is observed that proposed scheme performs better than existing scheme. Proposed scheme EAACK surpassed existing systems when number of malicious nodes increased in the network. From these results it is conclude that proposed system has greater performance than existing TWOACK, AACK scheme. From the result, it is conclude that acknowledgment-based scheme EAACK is able to detect misbehaviour with the presence of receiver collision and limited transmission power.

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. 3, Issue 4, April 2015

C. Simulation Result –Scenario 3

In terms of RO, owing to the hybrid scheme, EAACK maintains a lower network overhead compared to TWOACK in most cases, as shown in Figure 12 However, RO rises rapidly with the increase of malicious nodes. It is due to the fact that more malicious nodes require a lot more acknowledgment packets and digital signatures.
In the third scenario, all malicious nodes are set to send out false misbehaviour report to the source node whenever it is possible. This scenario setting is designed to test the IDS's performance under the false misbehaviour report. Fig. 13 shows the achieved simulation results based on PLR. When malicious nodes are 10%, EAACK performs 99% better than AACK and TWOACK. When the malicious nodes are at 20% and 30%, EAACK outperforms all the other schemes and maintains the PLR to over 99%. We believe that the introduction of MRA scheme mainly contributes to this performance. EAACK is the only scheme that is capable of detecting false misbehaviour report.

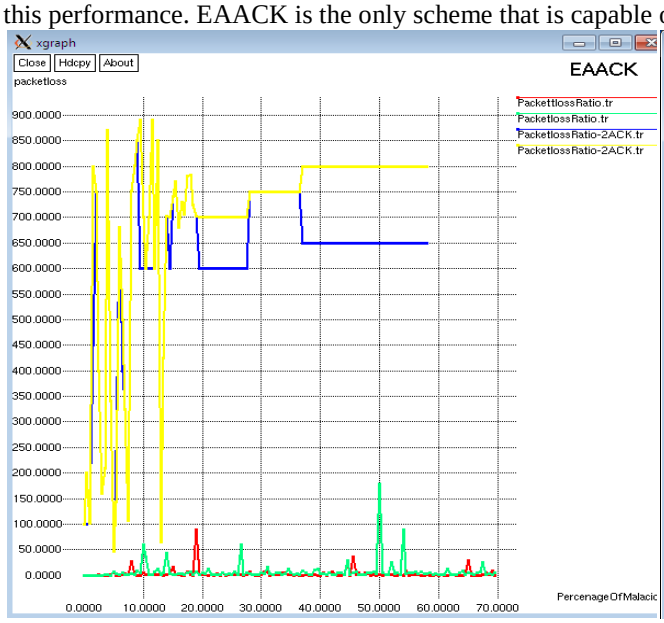

Fig 13.Simulation Result for Scenario 3:PacketLoss Ratio

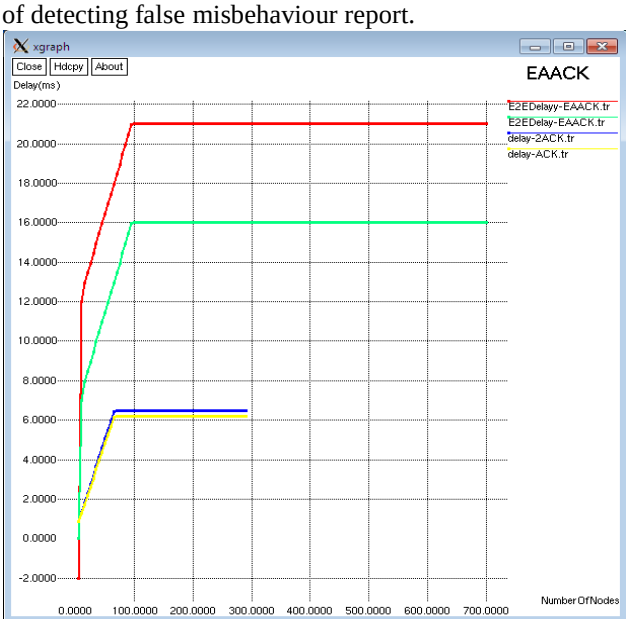

Fig 14 Simulation Results for Scenario 3-End-to-End Delay

VI. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANET. The dissertation work implements a IDS named EAACK specially designed for MANETs and compared it against other popular mechanism in different scenarios through simulations. The result demonstrated positive performance against Watchdog, TWOACK and AACK in case of receiver collision, limited transmission and false misbehaviour attack.

To prevent attackers from the initiating forged acknowledgment attacks, digital signature scheme is incorporated in proposed scheme EAACK. Although it generates more routing overhead in some cases, it can vastly improve the networks PLR when attackers are smart enough to forge acknowledgment .In order to seek optimal DSAs for both DSA and RSA schemes are implemented in simulation. Eventually arrived to the conclusion that DSA scheme is more suitable to be implemented in MANETs.
The results of graphs are shown in above Table I

REFERENCES

1. Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami, "EAACK- A Secure Intrusion Detection System for MANETs," IEEE Transactions on Industrial Electronics. Vol.60, no.3, MARCH, 2013.
2. Adnan Nadeem, Michael P. Howarth, "A Survey of MANET Intrusion Detection &
3. Prevention Approaches for Network Layer Attacks," IEEE Communication Surveys & Tutorial, Vol. 15, No. 4, Fourth Quarter 2013
4. R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

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. 3, Issue 4, April 2015

5. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.
6. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
7. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.
8. Michele Nogueira Lima, Aldri Luiz dos Santos, and Guy Pujolle, "A Survey of Survivability in Mobile Ad Hoc Networks," IEEE Communication Surveys & Tutorial, Vol. 11, No. 1, First Quarter 2009
9. T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.
10. Mike Burmester, Breno de Medeiros," On the Security of Route Discovery in MANETs,"IEEE Transactions On Mobile Computing, Vol. 8, No. 9, September 2009
11. V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind.Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.
12. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Transaction in Mobile Computing., vol. 6, no. 5, pp. 536–550, May 2007.
13. N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Communication., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159
14. L. Buttyan and J. P. Hubaux, "Security and Cooperation in Wireless Networks," Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
15. A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks,"Wireless Communications, IEEE, vol. 11, Feb 2004, pp. 48- 60.
16. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEE Workshop Mobile Computing. Syst. Appl, 2002, pp. 3–13.
17. Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23
18. S.Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Computing. Netw, Boston, MA, 2000, pp. 255–265.
19. Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," 6th Int'l. Conf.
20. Mobile Comp. And Net. Aug. 2000, pp. 275–83.

BIOGRAPHY

Trupti Ghongade did B.E in Information Technology from Amravati University, Dr.Sau Kamaltai Gawai College of Engg.& Technology, Amravati in 2012.She is pursuing for ME CSE from G.H. Raisoni, Amravati. Her research interest includes Networking,Network Security.

Prof. Avinash P. Wadhe did B.E from SGBAU Amravati University and M-Tech (CSE) From G.H Raisoni College of Engineering, Nagpur (an Autonomous Institute). He is currently an Assistant Professor with the G.H Raisoni College of Engineering and Management, Amravati SGBAU Amravati University. His research interest include Network Security, Digital forensics .He has contributed to more than 20 research paper.