ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

A Secure Intrusion Detection System for Manets by using Cryptographic Algorithms

K.Kirubani[1], S.P.Anbukodi[2]

PG Student [EST], Dept.of EEE, Krishnasamy College of Engineering and Technology,Cuddalore,Tamilnadu, India[1]

Assistant professor, Dept.of ECE, Krishnasamy College of Engineering and Technology, Cuddalore, Tamilnadu, India [2]

ABSTRACT: The migration to wireless network form wired network has been a worldwide trend within the past few decades. Among all the up to date wireless networks, Mobile Ad hoc Network (MANET) is one amongst the foremost necessary and distinctive applications. On the contrary to ancient specification, MANET doesn't need a set of network infrastructure; each single node works as each a transmitter and a receiver and they trust their neighbors to relay messages. Nodes communication directly with one another once they are in range intervals constant communication varies. The self-configuring ability of nodes in MANET created it fashionable among vital mission applications like military use or emergency recovery. Unfortunately, the open medium and remote distribution of MANET create it at risk of numerous kinds of attacks. So, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. MANET into industrial applications. In this project, we define solid privacy requirements regarding malicious attackers in MANET. Then we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

KEYWORDS: Digital signature, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgement(EAACK), Mobile Ad hoc Network(MANET).

I.INTRODUCTION

Due to their natural quality and scalability, wireless networks area unit perpetually most popular since the primary day of their invention. Because of their improved technology and reduced costs, wireless networks have gained rather more preferences over wired networks in the past few decades. Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and receiver that communicate with each other. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their quality. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the nodes is beyond the communication range. MANET solves this drawback by permitting intermediate parties to relay information transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In single-hop, all the nodes within the same radio range communicate directly with each other. On the opposite hand, in multihop network, nodes admit different intermediate nodes to transmit if the destination node is out their radio vary. MANET is capable of making a self-configuring and self-maintaining network while not the assistance of a centralized infrastructure, that is commonly unfeasible in crucial mission applications like military conflict or emergency recovery.Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks.Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

II.BACKGROUND

A. Intrusion Detection System in MANETs

Due to the limitation of most MANET routing protocol, nodes in MANETs assume that other nodes always cooperate with each other to relay data. 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 MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

completely eliminate the potential damages caused by compromised nodes at the first time. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK, and Adaptive ACKnowledgement.

1) Watchdog: the Watchdog scheme is consisted of two elements, namely, Watchdog and Pathrater. Watchdog detects malicious misbehaviors by promiscuously being attentive to its next hop's transmission. If a watchdog node overhears that its next node fails to forward the packet among a particular amount of your time, it will increase its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. Moreover, compared to another schemes, Watchdog is capable of police investigation malicious nodes instead of links. The watchdog theme fails to observe malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) restricted transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping. We tend to discuss these weaknesses with additional detail in Section III.

2) TWOACK: With respect to the six weaknesses of the Watchdog theme, several researches projected new approaches to unravel these problems. TWOACK detects misbehaving links by acknowledging each information packet transmitted over each three consecutive nodes on the trail from the supply to the destination. TWOACK is needed to figure on routing protocols like Dynamic SupplyRouting. The operating method of TWOACK is shown in Fig. 1: Node A primary forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. Once node C receives Packet 1, because it is two hops from node A, node C is duty-bound to come up with a TWOACK packet, that contains 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 one from node A to node C is fortunate. Otherwise, if this TWOACK packet is not received in an exceedingly predefined period, each nodes B and C area unitreported malicious.Identicalmethod applies to each three consecutive nodes on the remainder of the route.

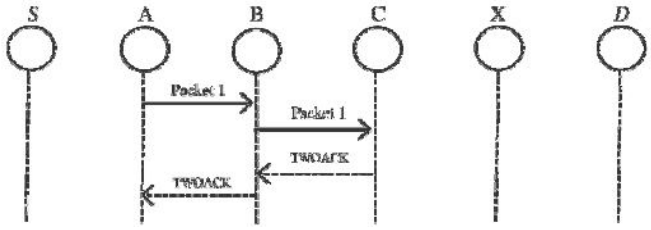

Fig.1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

3) AACK: It is based on TWOACK, proposed a new scheme called AACK. Almost like TWOACK, AACK is an Adaptive Acknowledgment-based network layer scheme which may be considered as the combination of a scheme called TWOACK associated an end-to-end acknowledgment scheme referred to as ACKnowledge. Compared to TWOACK, AACK considerably reduced network overhead whereas still capable of maintainingsurpassing identical network output. The end-to-end acknowledgment theme in ACK is shown in Fig. 2.the supply node S sends out Packet

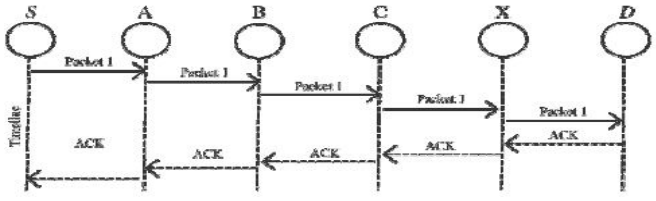

Fig.2. ACK scheme: The destination node is required to send acknowledgment packets to the source node.

one with none overhead except two b of flag indicating the packet sort. All the intermediate nodes merely forward this packet. Once the destination node D receives Packet one, it is needed to challenge associate ACK acknowledgment packet to the supply node S on the reverse order of identical route. Among a predefined period, if the supply node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is fortunate. Otherwise, the supply node S can switch to TACK scheme by causation out a TACK packet. The conception of adopting a hybrid theme in AACK greatly reduces the network overhead, however each TWOACK and AACK still

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

suffer from the matter that they fail to observe malicious nodes with the presence of false misbehaviors report and forged acknowledgment packets.

B. Digital Signature

Digital Signature has continually been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. The pursuit of secure communication has been conducted by person since 4000 years ago in Egypt, and in keeping with Kahn's book in 1963. Such development dramatically accelerated since the World War II, which some believe is largely due to the globalization or economic process.

The security in MANETs is outlined as a mix of processes, procedures, and systems used to ensured confidentiality, authentication, integrity, availability, and nonrepudiation. Digital signature may be a wide adopted approach to confirm the authentication, integrity, and nonrepudiation of MANETs.

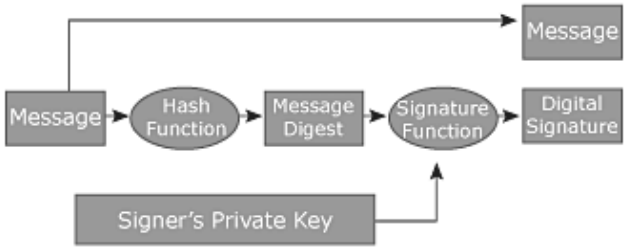

Fig.3. Communication with digital signature.

To ensure the validity of the digital signature, the message is send to the hash function or if the message is valid data means it directly send to the messages, and the hash function is processed and then it sender to the message digest, the message digest is used to check the message whether the message is valid or not. And then it sender to the signature function, it check signature is private key or public key. To verify the signature by applying public key or private key by using generalized as an information string.

III.PROBLEM IDENTIFICATION

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. In this section, we discuss the three weaknesses in detail.

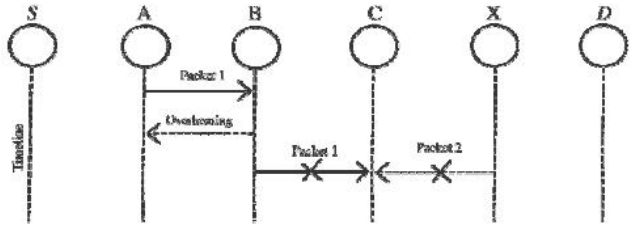

Fig.4. Receiver collisions: Both nodes B and X are trying to send Packet1 and Packet2, respectively, to node C at the same time.

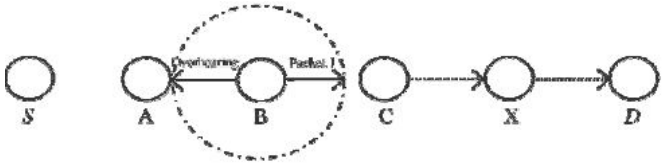

Fig.5. Limited transmission power: Node B limited transmission power so that the packet transmission can be overhead by node A but too weak to reach node C.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

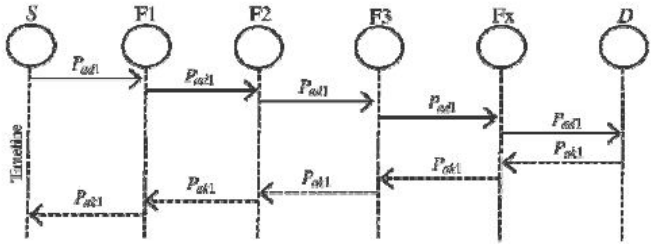

Fig.6.System controller flow: This figure show system flow the EAACK scheme works.

In a typical example of receiver collisions, shown in Fig. 4, once node A sends Packet one to node B, it tries to take in if node B forwarded this packet to node C; in the meantime, node X is forwarding Packet a pair of two node C. In such case, node A overhears that node B has with success forwarded Packet one to node C however did not observe that node C failed to receive this packet as a result of a collision between Packet one and Packet a pair of at node C.
In the case of restricted transmission power, so as to preserve its own battery resources, node B on purpose limits its transmission power in order that it is robust enough to be overheard by node A however not robust enough to be received by node C, as shown in Fig. 5.

For false wrongful conduct report, though node A with success overheard that node B forwarded Packet one to node C, node A still rumoured node B as misbehaving, as shown in Fig. 6. As a result of the open medium and remote distribution of typical MANETs, attackers will simply capture and compromise one or 2 nodes to attain this false wrongful conduct report attack.

IV.PROPOSED SYSTEM

EAACK is consisted of three major components, namely, ACK, secure ACK, and misbehavior report authentication. In order to distinguish different packet varieties in different schemes, we tend to enclose a 2-b packet header in EAACK.

A. ACK

ACK is essentially associate end-to end acknowledgment scheme. It acts as a district of the hybrid scheme in EAACK, attending to scale back network overhead once no network misconduct is detected. In Fig. 8, in ACK mode, node S initial sends out associate ACK information packet P_{ad1} to the destination node D. If all the intermediate nodes on the route between nodes S and D square measure cooperative and node D with success receives P_{ad1}, node D is needed to remand associate ACK acknowledgment packet P_{ak1} on a similar route however in a very reverse order. Inside a predefined fundamental quantity, if node S receives P_{ak1}, then the packet transmission from node S to node D is winning. Otherwise, node S can switch to S-ACK mode by causing out associate S-ACK information packet to sight the misbehaving nodes within the route.

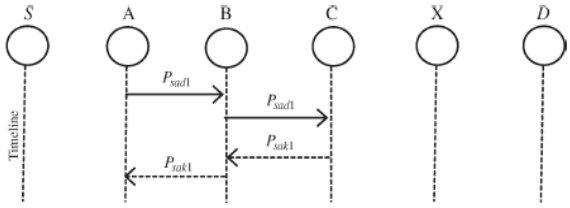

Fig.7. ACK scheme: The destination node is required to send back an acknowledgement packet to the source node when it receives a new packet.

B. *S-ACK*

The S-ACK scheme is associate improved version of the TWOACK scheme projected by Liu et al. The principle is to let each three consecutive nodes work in a group to sight misbehaving nodes. For each three consecutive nodes within the route, the third node is needed to send associate S-ACK acknowledgment packet to the primary node. The intention of introducing S-ACK mode is to sight misbehaving nodes within the presence of receiver collision or restricted transmission power.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

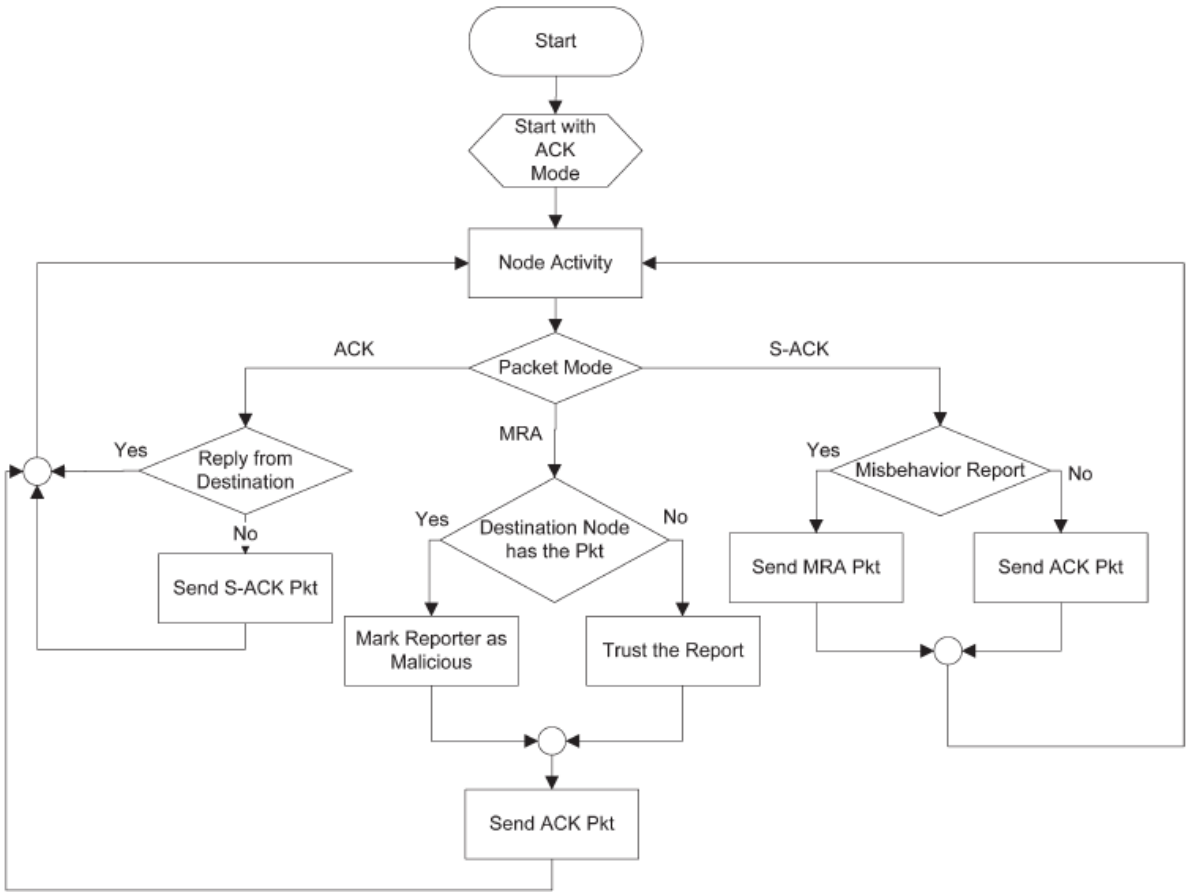

Fig.8. S-ACK scheme: Node C is required to send back an acknowledgment packet to node A.

As shown in Fig. 8, in S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) add a group to sight misbehaving nodes within the network. Node F1 initial sends out S-ACK information packet P_{sad1} to node F2. Then, node F2 forwards this packet to node F3. Once node F3 receives P_{sad1}, because it is that the third node during this three-node cluster, node F3 is needed to remand associate S-ACK acknowledgment packet P_{sak1} to node F2. node F2 forwards P_{sak1} back to node F1. If node F1 doesn't receive this acknowledgment packet inside a predefined fundamental quantity, each node F2 and F3 square measure rumoured as malicious. Moreover, a misconduct report are generated by node F1 and sent to the supply node S. In TWOACK theme, wherever the supply node like a shot trusts the misconduct report, EAACK needs the supply node to modify to MRA mode and make sure this misconduct report.

C. MRA

The MRA scheme is used to resolve the weakness of Watchdog once it fails to sight misbehaving nodes with the presence of false misconduct report. The false misconductreport may be generated by malicious attackers to incorrectly report innocent nodes as malicious. The core of MRA scheme is to attest whether or not the destination node has received the reported missing packet through a special route. Once the destination node receives associate MRA packet, it searches its native knowledge base and compares if the reported packet was received. Otherwise, the misconduct report is trusty and accepted. By the adoption of MRA theme, EAACK is capable of sleuthing malicious nodes despite the existence of false misbehavior report.

D. Digital Signature

As mentioned before, EAACK is associate acknowledgment based IDS. All three components of EAACK, namely, ACK, S-ACK, and MRA, square measure acknowledgment-based detection schemes. All of them believe on

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

acknowledgment packets to sight misbehaviors within the network. Otherwise, if the attackers square measure good enough to forge acknowledgment packets, all of three schemes will be vulnerable.

With reference to this imperative concern, we tend to incorporated digital signature in our projected theme. So as to make sure the integrity of the IDS, EAACK needs all acknowledgment packets to be digitally signed before they are sent out and verified till they're accepted.

V. SIMULATION METHODOLOGY

In this section, we concentrate on describing our simulation environment and methodology as well as comparing performances through simulation result comparison with Watchdog, TWOACK, and EAACK schemes.

A. Simulation Methodologies

To better investigate the performance of EAACK underneath different kinds of attacks, we tend to propose three scenario settings to simulate different types of misbehaviors or attacks.

Scenario 1:During this scenario, we tend to simulate a basic packet dropping attack. Malicious nodes merely drop all the packets that they receive. The main of this situation is to check the performance of Intrusion-Detection System (IDS) against two weaknesses of Watchdog, namely, receiver collision and limited transmission power.

Scenario 2: This scenario is meant to check IDSs' performance against false misbehavior report. During this case, malicious nodes continuously drop the packets that they receive and send back a false misbehavior report whenever it is possible.

Scenario 3: In this scenario, to check the IDSs' performance when the attackers are smart enough to forge acknowledgment packets and claiming positive result whereas, in fact, it is not positive. As Watchdog is not associate acknowledgment-based scheme.

B. Simulation Configurations

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform and Ubuntu 10.04. The system is running on a laptop with Core™2 Duo T6400 CPU and 1GB RAM. In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.34. The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670 × 670 m. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS 2.34. The moving speed of mobile node is limited to 20 m/s and a pulse time of 1000 s. UDP traffic with Constant Bit Rate (CBR) is implemented with a packet size of 512 bytes. In order to measure and compare the performance of our proposed scheme, we continue to adopt the following two performance metrics:

- *Packet Delivery Ratio (PDR):* Packet Delivery Ratio defines the ratio of the number of packets received by the destination node and the number of packets sent by the source node.
- *Routing Overhead (RO):* Routing Overhead defines the ratio of the amount of routing-related transmission (RREQ, RREP, RERR, ACK, S-ACK and MRA).

During the simulation, the source route broadcasts a Route REQuest (RREQ) message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcast this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a Route ERRor (RERR) message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates a RouteREPly (RREP) message and sends this message back to the source node by reversing the route in the RREQ message.

Regarding the digital signature schemes, we adopted an open source library named Botan. This cryptography library is locally compiled with GCC 4.3. To compare performances between DSA and RSA scheme, we generated 1024 bit DSA key and 1024 bit RSA key for every node in the network.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

We assumed that both a public key and a private key are generated for each node and they were all distributed in advance. Typical size of public key and private key file is 654 bytes and 509 bytes with a 1024 bit DSA key respectfully. On the other hand, the size of public key and private key file for 1024 RSA is 272 bytes and 916 bytes respectively. The signature file size for DSA and RSA is 89 bytes versus 131 bytes respectively.

C. Performance Evaluation

To provide readers with a better insight on our simulation results. In simulation results, we use eleven nodes and zero is the source node and then two is the destination node. Here, the source node will send the communication signal to all the node i.eshown in fig.9.

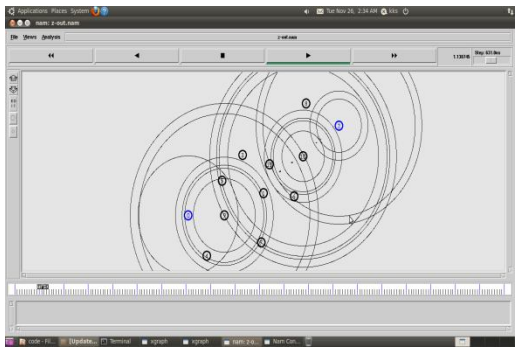

Fig.9.Source node sends communication signal to the destination node

If the source node has no route to the destination node, then the source node initiates the route discovery in an on-demand fashion. After generating RREQ, node looks up its own neighbour table to find if it has any closer neighbour node toward the destination node. If a closer neighbour node is available, the RREQ packet is forwarded to that node. If no closer neighbour node is the RREQ packet is flooded to all neighbour nodes. And the source node will send the packet to the destination node and then the destination node RREP to the source node. And thenAttack issues will arise to thenetwork, providing security to the attacks will be considered. MANETs face different securities threats i.e. attack thatarecarried out against them to disrupt the normal performance of the networks.

In existing system, the source will send the data to the destination node. For that, the source node will send the communication signal to the entire node. So the neighbour node will reply request to the source node. And then only the source node will send the data to the destination node through some of the nodes. In a particular time interval the data will sends. Unfortunately, some set of node act as the hackers' node. For that, the malicious nodes drop all the packets that pass through it. That is shown in fig.9.

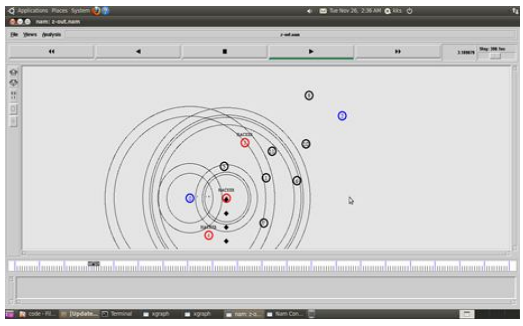

Fig.10.Source node sends data to the destination node, without knowing the presence of hackers.

The packet delivery ratio and the routing overhead in TWOACK are shown in fig.10 and fig.11. X axis is number of time and Y axis is number of packet delivery ratio, the source node sends data to the destination node, without knowing the presence of hackers. In zeroth time onwards, the process will start. At the time the action will performed and in

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

particular interval time, it find the hacker node. So it drops the entire packet without knowing the presence of the hacker and no routing overheads is there.

In proposed system, we use eleven nodes and zero is the source node and then two is the destination node. Here, the source node will send the communication signal to the entire node.

If it finds the neighbor node and then the source node will send the packet to the destination node. If it finds the hacker node means, certainly it transfers the path i.e. shown in figure 12 and 13.

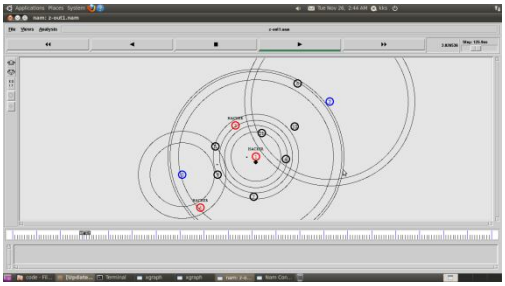

Fig.12.Source node is find the hacking while sending the node to the destination node

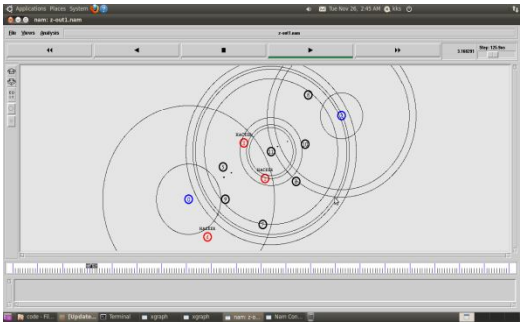

Fig.13. After found the hacker, the transmission path has been changed

Fig.14 and 15 is mention that routing overhead and packet delivery ratio. In that, it founds the hacker, so the node can be continuously delivering the packet easily and also overcomes the routing overhead.

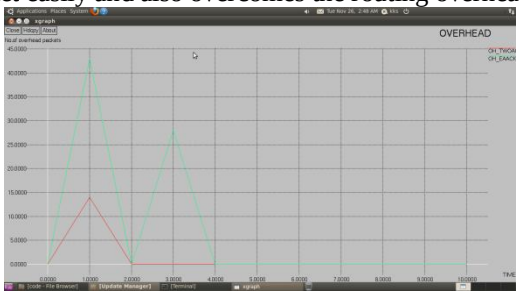

Fig.14.Comparison output of Overhead in EAACK

The routing overhead in TWOACK, it cannot find the hacker, because for the overhead will appearing till the process is running, but in EAACK, it easy to found the hackers by using digital signature, so it overcome the routing overhead. i.e shown in fig.14.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

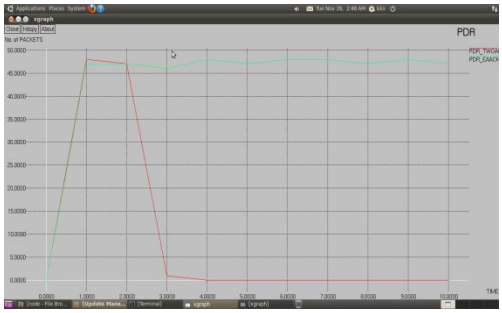

Fig.15.Comparison output of Packet Delivery ratio in EAACK

The packet delivery ratio in TWOACK, it cannot find the hacker, so minimal packet delivery ratio function will process. And in the EAACK, it easy to found the hackers by cryptographic algorithms, so the packet delivery ratio is high.

VI.CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. We think that this tradeoff is worthwhile when network security is the top priority.

In EAACK unfortunately we were selecting malicious node as an intermediate node, then we finding and rectify the problem, future, if any malicious node enter the network region, we simply ignore the node while selecting intermediate nodes

REFERENCES

[1] 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.
[2] 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.
[3] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.
[4] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in *Proc. IEEE Int.Conf. Commun.*, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.
[5] G. Jayakumar and G. Gopinath, "*Ad hoc* mobile wireless networks routing protocol—A review," *J. Comput.Sci.*, vol. 3, no. 8, pp. 574–582, 2007.
[6] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in *Proc. IEEE Int. Conf.Perform., Comput., Commun.*, 2004, pp. 747–752.
[7] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshopMobile Comput. Syst. Appl.*, 2002, pp. 3–13.
[8] L. Zhou and Z. Haas, "Securing ad-hoc networks," *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.
[9] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.
[10] 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. 813–819, Mar. 2010.
[11] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.
[12] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science,vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.
[13] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.
[14] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in *Proc. 2nd Conf. m-Bus.*, Vienna, Austria, Jun. 2003.
[15] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," *IEEETrans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.
[16] M. Zapata and N. Asokan, "Securing *ad hoc* routing protocols," in *Proc.* ACM Workshop Wireless Secur., 2002, pp. 1–10.