ISSN:0975-9646

A Novel Key Exchange Mechanism for Secure Intrusion-Detection System for MANET

D.Anil[1],Dr. S. Vasundra[2]
[1]*Dept. Of Computer Science & Engineering, JNTUACEA, Anantapuramu (515002), Andhra Pradesh, India*
[2] *Professor, CSE Department, JNTUACEA, Anantapuramu (515002), Andhra Pradesh, India*

ABSTRACT: WIRELESS NETWORKS HAS BECOME THE MOST POPULAR COMMUNICATION MEDIA NOW A DAY. APART FROM THE PERFORMANCE, THE MOBILITY AND SCALABILITY ISSUES, MADE THE WORLD TO MIGRATE TO THE WIRELESS NETWORKS FROM WIRED NETWORK. AMONG ALL THE WIRELESS NETWORKS THE MOBILE ADHOC NETWORK IS THE MOST POPULAR AND UNIQUE ONE. IN CONTRAST WITH THE TRADITIONAL NETWORK ARCHITECTURE, MANET DOES NOT HAVE A FIXED INFRASTRUCTURE. THE NODES IN THE MANET ARE SELF-CONFIGURING NODES, EVERY NODE ACT AS A RECEIVER AS WELL AS TRANSMITTER WHEN NEEDED. A NODE NEEDS TO COMMUNICATE WITH ANOTHER NODE, THEY CHECK FOR THE COMMUNICATION RANGE, IF THE NODE IS WITHIN THE COMMUNICATION RANGE, THEN COMMUNICATION OCCURS DIRECTLY. OTHERWISE THEY DEPEND ON THEIR NEIGHBOURING NODES TO RELAY THE MESSAGE. MANETS HAVE A WIDE RANGE OF APPLICATIONS LIKE MILITARY USE AND IN EMERGENCY SITUATIONS, BECAUSE OF THIS SELF-CONFIGURING NATURE. THE NODES IN THE MANETS ARE DISTRIBUTED RANDOMLY OVER THE NETWORK AND ANY NODE CAN ENTER AND LEAVE THE NETWORK, DUE TO THESE REASONS THE NETWORK IS VULNERABLE TO ATTACKS. HENCE IT IS CRUCIAL TO DEVELOP AN INTRUSION DETECTION SYSTEM. IN THIS PAPER, A MECHANISM CALLED ENHANCED ADAPTIVE ACKNOWLEDGEMENT (EAACK) ALONG WITH AN ENCRYPTION TECHNIQUE, SHA1 IS IMPLEMENTED.

KEYWORDS: INTRUSION DETECTION SYSTEM, EAACK, MANET, SHA1

I. INTRODUCTION

With the wide spread of laptops and Wi-fi, wireless networking have made MANETs a popular research topic since the mid-1990s.A Mobile Ad Hoc Network (MANET) is a self-configuring network of mobile routers connected by wireless links - the union of which form a. The routers are free to move randomly and organize themselves[1]; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced disasters, military conflicts, emergency medical situations[2] etc.

The nodes in the MANET are mobile i.e. they can move independently in any direction and therefore the links between two nodes may not remain for long time. Each node acts as both transmitter and receiver.Nodes are free to move arbitrarily, thus the network topology may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links. The communication in MANETs generally happens in two ways single hop and multi hop. When two communicating nodes are within the same radio range, they communicate directly. Otherwise they depend on the neighbouring nodes to relay the messages. The nodes that relay messages in this case acts as routers. Hence nodes in a MANET acts as a transmitter, receiver as well as router.

MANETs have a decentralized infrastructure, and hence any node can enter or leave the network without any authorization in to the network. The nodes in the MANETs are self-configuring and self-maintaining. MANETs do not have a fixed infrastructure and a centralised base station, they define their own configurations, infrastructure and topology so, the nodes are always free to move. Due to these features, MANETs usage is spreading globe wide. The applications of MANETs include military, in emergency situation where a particular fixed infrastructure is no possible, medical field. As MANETs need very little configuration and self maintaining capability they can be used in human induced disasters, medical emergency situations.

Because of these unique characteristics of MANETs, they are almost used everywhere. Unfortunately, due these characteristics they are vulnerable to attacks. Intruders may enter the network and disclose the information in the network. Prevention of intruders to enter the network is costly and almost impossible and hence some intrusion detection system should be included in the network to find the malicious nodes in the network and eliminate them from the network.

II. BACKGROUND

A. IDS in MANET

The nodes in the MANETs cooperate each other because of the characteristics of MANETs. This leaves the attackers a loop hole to enter into the network and compromise the whole network. It is better to detect the nodes malicious behaviour immediately after entering the network. By detecting the intruders at the beginning, the damage to the network can be minimised to a greater extent. Hence an Intrusion Detection System is a must and should mechanism included in any network. The Intrusion Detection System however acts second layer where as the routing protocol will be the first layer in the communication process of MANETs.

Many researchers proposed many schemas for the Intrusion Detection. Among them three main schemas discussed below

1) Watchdog: The Watchdog schema is proposed by Marti *et al.* [3], it aims to improve the throughput of the system even in the presence of malicious nodes. There will be two parts in this schema namely: Watchdog and Pathrater. The watchdog will be observing every hop transmission; it increases the count value of a node if there is any failure in the transmission from that node to another node. When the count reaches a particular threshold value then watchdog reports that node as malicious. The pathrater works along with the routing protocol by avoiding the malicious node to communicate with other nodes in the network.

2)TWOACK: TWOACK, proposed by Liu *et al.* [4], is not an extension for the Watchdog. TWOACK detects the misbehaving[8] links by considering the acknowledgments of every three consecutive nodes in the network. The process goes on like this as shown in Fig 1 the node n1 sends a packet to node n2 and node n2 forwards that to node n3. As soon as node n3 receives the data packet it should send the TWOACK packet to node n1 in the reverse route. If node n1 receives the TWOACK packet then the transmission from n1 to n3 is successful. Otherwise nodes n2 and n3 are reported as malicious nodes. The process is repeated for every three consecutive nodes in the whole network.

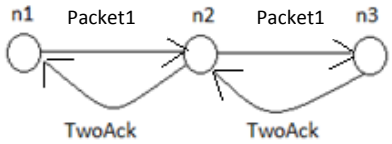

Fig 1. TWOACK Schema

B. Digital Signature

Most of the Intrusion Detection Systems depend on acknowledgments and hence the acknowledgments are to be validated. It is very important assure that the acknowledgment packets are valid. So, the acknowledgments are to be digitally signed. A new schema called Enhanced Adaptive ACKnowledgment is proposed in which the digital signatures are adopted.

In MANETs, security will be having the first priority. The system should ensure security issues like authentication, integrity and nonrepudation[6], which can be done by adopting digital signatures. Elhadi M. Shakshuki adopted RSA[10] and DSA[5] algorithm for addressing the security issues. In RSA[10] algorithm the sender and receiver will be having two keys namely: public key and private key; the private key will not be revealed, where as public key will be shared between the sender and receiver. Messages will be encrypted and decrypted using the public key and private key. Vs the messages are encrypted they can also be transferred via unsecured channel.

III. PROPOSED SCHEME

A. EAACK

In the proposed system, SHA1[9] algorithm is adopted for Enhanced Adaptive ACKnowledment(EAACK). EAACK consists of three major parts: ACK, Secure ACK(S-ACK), Misbehaviour Report Authentication (MRA). Adhoc On Demand Vector(AODV) is used as the routing protocol. AODV protocol eliminates the count-to-infinity problem, which a major problem in many other routing protocols.

1) ACK: ACK is generally, traditional end to end acknowledgment schema. Data packets are sent from source to destination and acknowledgment packets are sent back in the reverse path from destination to source. It is a part of EAACK schema, to reduce the network overhead with assumption that there is no malicious nodes in the network. As shown in the Fig 2 data packet are sent from s to d along the path s→n1→n2→n3→d. Immediately after d receives the data packet, d sends ack packet back to s in the reverse direction d→n3→n2→n1→s. if s receives the ack packet then the communication is successful. Otherwise s switches to S-ACK by sending S-ACK packet to detect the malicious node.

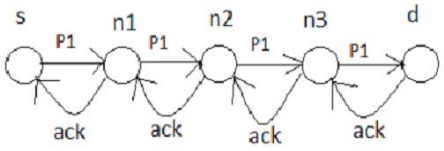

Fig 2. ACK Schema

2) Secure-ACK: The S-ACK schema is improvement of TWOACK schema proposed by Liu *et al.* The working of this schema is similar to the TWO ACK, in which three consecutive nodes are considered for detecting the malicious node. Consider three consecutive nodes A,B, C. Node A send a data packet to Node B, which will be forwarded to node C. When there are no malicious nodes Node C sends back S-ACK packet to node B and then the S-ACK forwarded to node A, which is a successful transmission. On the other hand, if node A did not receive S-ACK packet before a certain amount of time, unlike TWOACK it switches to MRA Schema, where the misbehaviour report is reviewed.

3) MRA: Misbehaviour Report Authentication schema is for avoiding the false misbehaviour report, which is generated by the malicious nodes to mislead the network by reporting the innocent nodes as malicious nodes. The MRA schema checks the local knowledge base of source node for alternative route to the destination. If the data packet reaches the destination through any other alternative route then the misbehaviour report generated previously is distrusted otherwise the node that reported the misbehaviour is declared as malicious node.

The whole process of EAACK schema is described using a flowchart show in Fig 3.

B. Generating Message Digests

Every part of EAACK; ACK, S-ACK, MRA are acknowledgment based schemes. The whole communication is depending on the acknowledgment.

The acknowledgments can be forged[11] by the malicious nodes which will compromise the whole network. For every acknowledgment packet a message digest is generated.SHA1 algorithm, which uses hash function for generating message digests of data packets and acknowledgment packets in all the three sub parts of EAACK.

The message is padded with 1's and 0's such that its length is a multiple of 64. Then the message is encrypted using a hash function. SHA1 requires 80 processing functions and 80 processing constants for generating the message digest.

IV. PERFORMANCE ANALYSIS

The simulation of the network is carried out in Network Simulator 2.34 on ubuntu 10.14 platform.

The main aim of the system is secure communication, i.e to check whether the data packets are delivered or not by eliminating the malicious nodes. So, Packet Delivery Ratio is considered as the metric to measure the performance of the network using EAACK.

Packet Delivery Ratio is defined as the ratio of number of packets received by the destination to the number of packets sent by the source.

$$PDR = \frac{\text{No. of data packets received}}{\text{No. of data packets sent}}$$

In simulation AODV Routing protocol is used as it eliminates the count-to-infinity problem. The source node broadcasts the RREQ packet to all its neighbours. All the neighbours, upon receiving this packet appends their respective addresses along with sequence number is forwards the RREQ packet to their corresponding neighbours. This continuos until the RREQ packet is received by the destination. The RREQ packet sent to a neighbour only if the sequence number of that node is greater than the sequence number of sender node. This eliminates the infinite loops in the network which in turn reduces the routing overhead.

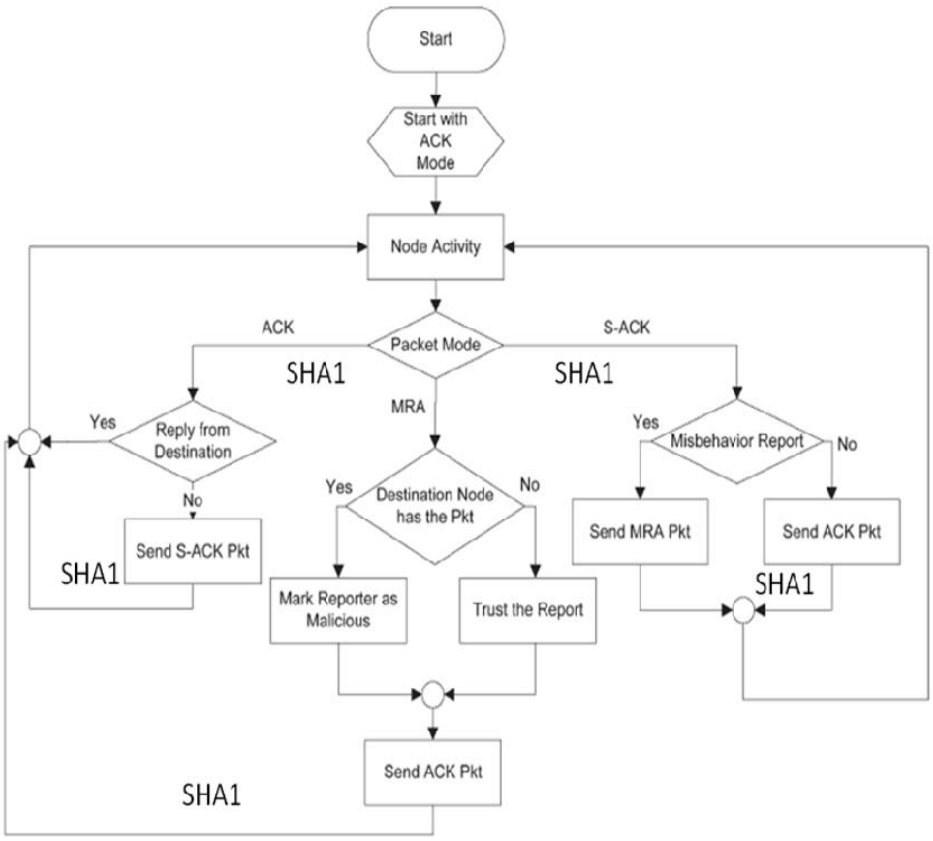

Fig 3 Enhanced Adaptive Acknowledgement Schema with SHA1 Algorithm

V. RESULTS

Graphs are used to visualise the performance improvement of the proposed scheme. Xgraph is used to generate the graphs for the proposed work.

The graph is drawn for Packet Delivery Ratio against number nodes. Packet Delivery Ratio is calculated by changing the number nodes in the network. The packet delivery ratio decreased as number of nodes increased. As number of nodes increases, the number of malicious nodes may increase results in packet drops which leads to decrease in packet deliver ratio.

A comparison graph, based on values in Table 1 is generated for the SHA1 algorithm and RSA[10] algorithm. With the SHA1 algorithm the packet delivery ratio is a little bit higher than the packet.

Table 1 comparison of Packet Delivery Ratio for RSA and SHA1

Packet Delivery Ratio						
No. of nodes	18	20	25	30	33	35
EAACK (RSA)	0.22	0.19	0.15	0.11	0.098	0.096
EAACK (SHA1)	0.22	0.19	0.16	0.14	0.106	0.100

The comparison graph is shown in Fig 4

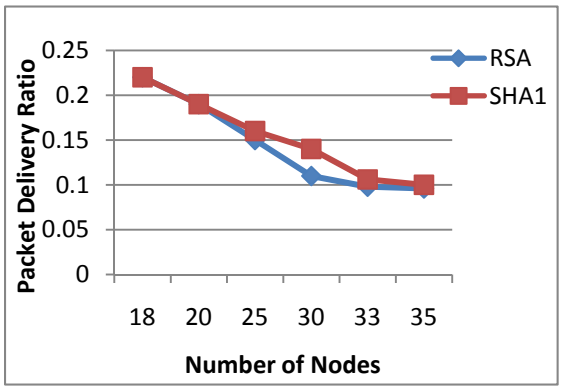

Fig 4 PDR Comparison between RSA and SHA1

The other comparison between the DSR and Adhoc On Demand Vector routing algorithm.

The number of packets lost is less in AODV routing protocol when compared with DSR routing protocol with constant simulation time.

Fig 5 shows numbers of packets received and number of packets lost with 10 seconds simulation time in the network using AODV algorithm.

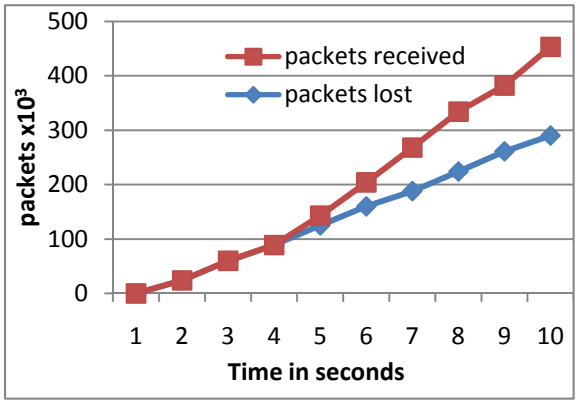

Fig 5 xgraph of 10 seconds simulation time

Fig 6 shows numbers of packets received and number of packets lost with 10 seconds simulation time in the network using DSR[5] algorithm.

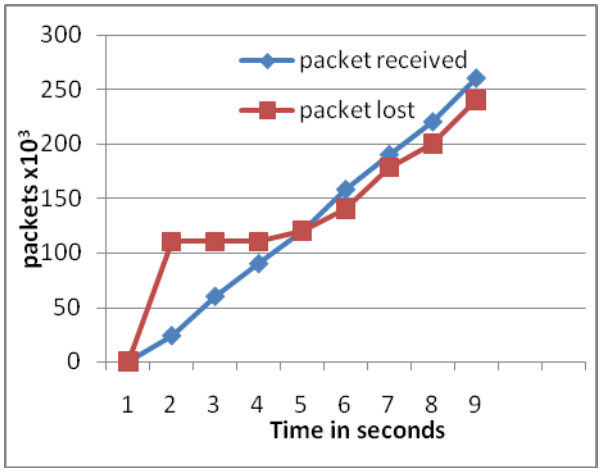

Fig 6 xgraph of 10 seconds simulation time

VI. CONCLUSION

The proposed scheme focuses on detection of misbehaving nodes and improves the packet delivery ratio by eliminating the malicious nodes. The packet delivery ratio is improved by using SHA1 algorithm instead of RSA[10] algorithm count of packets lost is decreased by using AODV instead of DSR routing protocol. By using AODV protocol the network overhead may increase due to the sequence numbers, but as the packet lose count increase the network overhead issue can be kept aside.

REFERENCE

[1] 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.

[2] M. Zapata and N. Asokan, "Securing *ad hoc* routing protocols," in *Proc.ACM Workshop Wireless Secur.*, 2002, pp. 1–10.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in Mobile Ad Hoc Networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265

[4] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[5] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[6] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of AppliedCryptography. Boca Raton, FL: CRC, 1996, T-37.

[7] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[8] 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.

[9] en.wikipedia.org/wiki/sha1

[10] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digitalsignatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.

[11] 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.

[12] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. heltami, "***EAACK—A Secure Intrusion-Detection System for MANETs***" IEEE Transactions on industrial electronics, vol. 60, no. 3, march 2013