Improved Acknowledgement Based Intrusion Detection System for Secured Transmission in MANETs

[1.] SowmyaSree. R, [2.]Ushanandhini. D. R, [3.]Kalaivani. S, [4.]S. Sivanantham
[1,2,3].Student, Dept of IT,ACE
[4.]Assistant Professor, Dept of IT

***Abstract*— The MANET in wireless sensor networks is preferred because of its mobility and scalability. This makes the use of MANETs in wide range of applications. The important criteria of the MANETs are its decentralized architecture. It does not require fixed infrastructure such as a base station for its operation. Instead it requires mobile nodes for transmitting the messages among the network. MANET is a collection of nodes connected with a wireless links either directly or indirectly. These nodes have ability to communicate among themselves by maintaining their mobility. Another important criteria of MANETs is its ability of self configuring. The major drawback of the MANETs is its open medium and remote distribution which allows intruder to easily insert the malicious nodes on to the network. Because of the decentralized architecture of MANETs it is difficult to develop IDS.**

I. Introduction

The wireless networks are preferred because of their improved technology and reduced cost. The Mobile Adhoc NETwork is a collection of nodes connected with wireless links either directly or indirectly. Each node in this network acts as a transmitter and receiver. These nodes communicate with each other through the wireless links. In wireless networks the nodes can communicate with each other only when the mobility is maintained, Which means that two nodes cannot transfer the data with each other when they are beyond the communication range.MANET overcomes this problem by providing the intermediate nodes that relays the data transmission. This is possible by dividing the MANETs into two network categories namely; single hop and multi hop. In single hop network all the nodes within the same range can communicate with each other. In the multi hop network the nodes depend on the other intermediate nodes to transfer while the destination node is out of their range. MANETs does not require fixed infrastructure[9] but it requires cooperative nodes, for forming the environment of cooperative nodes every nodes is supposed to be a friendly node and should willingly transfer the messages to their destination. Each node works in peer to peer mode and acts as an independent router that produces the independent data. The management of this transmission is distributed across the network. The open environment and remote distribution of MANET[4] makes it vulnerable to various types of attacks. Due to the lack of physical protection attackers can easily compromise the nodes and attack them[5].Because of decentralized architecture of MANETs it is difficult to develop an Intrusion Detection System (IDS).[6]

II. Intrusion detection in MANETs

A. *Types of Attacks*

The MANETs are exposed to the following types of attacks [13]:

i. Eavesdropping: The act of secretly listening to the private conversation of others without their concern.

ii. Wormhole: Packet is recorded at one location in the network and tunnels it to other location. This tunnel between colluding attackers is wormhole.

iii. Repudiation: This attack arises when an application does not adopt controls to properly track and log user’s actions, thus permitting malicious manipulation.

iv. Traffic analysis: The message contents are not obtained instead by tracking the frequency and length of the communication this information can be useful for identifying the nature of the communication.

v. Man in the middle attack: When the transmission of the message takes place between two parties the intruder attacks the transmission and the information is obtained from the transmission and modified and sent back again to the receiver.

B. *Intrusion Detection*

Network Based ID: monitoring Network traffic, packet flow and network infrastructure for anomalies and misuse.

Host Based ID: monitoring Computer processes and activities (nodes in the network) for Intrusion.

Whenever a Node in WSN is suspected to been attacked, the primary task is to identify the type of Intrusion and impact of Intrusion in the particular node and the secondary is to categorize the node as the following, based on its behaviour,

- Normal
- Abnormal but not Malicious
- Malicious

III. Existing System

A. *Watchdog*

Watchdog was mainly developed to improve the throughput of the network with the presence of malicious nodes. [14]There are two parts namely watchdog and pathrater. The watchdog are utilised for detecting the misbehaving nodes whereas pathrater is used to avoid routing of the packets that are transferred through the nodes in the network. For example in fig.1The watchdog overhears whether the PACKET1 is transferred successfully to node C by the node B, else the node B is marked as malicious. Watchdog maintains a buffer of recently transferred packets and compares each overhead packet with the packet in the buffer to check the similarity of the packet. If so the packet in the buffer is removed from buffer and forgotten by the watchdog. If the packet remains in the buffer for a long time than a certain timeout the watchdog increments the failure count for that node. If the threshold bandwidth exceeds a certain timeout then the watchdog notifies that node as malicious. The watchdog fails to detect the misbehaviours like: receiver collisions, limited transmission power and false misbehaviour report.

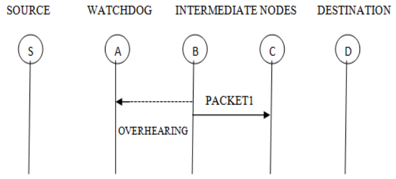

Fig 1. Watchdog

B. *TwoACK*

The TWOACK scheme [7] is a network layer technique to detect misbehaving links and to reduce their effects. In this scheme three consecutive nodes are considered and packets are transmitted from source to consecutive two nodes. After the acknowledgement is received then next three consecutive nodes are considered. TWOACK works on the routing protocol named Dynamic Source Routing (DSR). [8]The DSR protocol is used for routing packets between mobile hosts in an adhoc network. This protocol uses dynamic source routing which adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently. Based on the results from a packet level simulation of mobile hosts operating in an adhoc network, the protocol performs well over a variety of environmental conditions such as host density and movement rates. Due to the limited battery power nature of MANETs, such redundant transmission process can degrade the lifespan of the entire network.

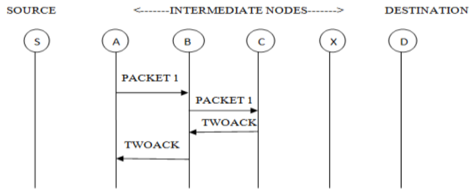

Fig 2. TwoACK

C. *Adaptive ACK*

(AACK) is acknowledgement based scheme. Compared to TWOACK, EEACK reduces network overhead. During transmission of the data in the EEACK scheme as in fig.3,if packet does not gets delivered successfully to the destination then the source node will switch to the TWOACK scheme by sending a TWOACK packet. Both EEACK and TWOACK detect the malicious node but trusts the misbehaviour report immediately.

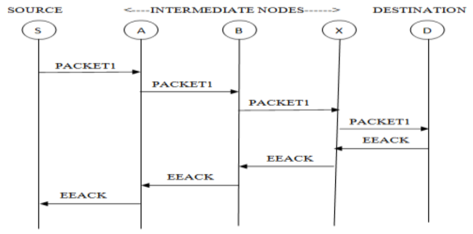

Fig 3. EEACK scheme

IV. Existing System

A. *Receiver Collisions*

When a node receives a packet from two other nodes at the same time then the receiver collision takes place. Example: After node A sends PACKET1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile node X is forwarding PACKET2 to node C. In such case, node A overhears that node B has successfully forwarded packet1 to node C and node C did not receive this packet due to a collision between PACKET1 and PACKET2 at node C.

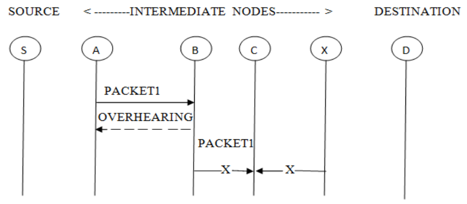

Fig 4. Receiver Collisions

B. *Limited Transmission Power*

A node knowingly limits its transmission power so that it is strong enough to be overheard by another node but not strong enough to receive any packets.

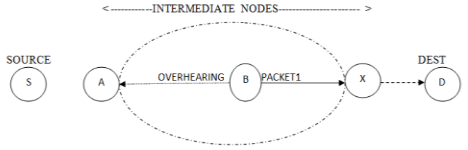

Fig 5. Limited Transmission Power

C. *False Misbehaviour Report*

If a node falsely reports that another node is misbehaving though that node has successfully forwarded the packet to the respective node, the false report is sent to the source by the malicious node.

For example in fig.6 Although node A successfully overheard that node B forwarded PACKET1 to node X, node A still reported node B as misbehaving. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehaviour report attack.

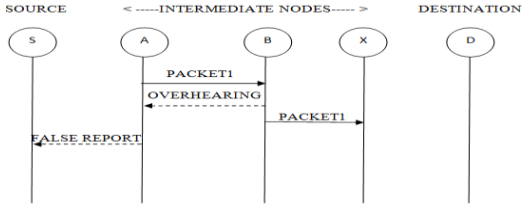

Fig 6. False Misbehaviour Report

V. PROPOSED SYSTEM

The existing works had some drawbacks such as receiver collisions, limited transmission power, false misbehaviour report, ambiguous collisions and failed to detect the malicious nodes for that purpose a new scheme IACK(Improved Acknowledgement Scheme) [1] is introduced and overcomes those drawbacks. IACK consists of four main parts namely:

- EEACK
- C-ACK (ConfidentialACK)
- MRA (MisbehaviourReportAuthentication)
- Schnorr Signature.

For distinguishing the different packet types in different schemes a 2-byte packet header is included in IACK. [6]

Table 1. Packet Type Indicators

PACKET TYPE	PACKET FLAG
General Data	00
ACK	01
S-ACK	10
MRA	11

A. *End to End ACK Scheme (EEACK)*

EEACK is an end-to-end acknowledgement scheme. [1] It acts as part of a scheme in IACK, designed for reducing network overhead when no network misbehaviour is detected. In EEACK the message is sent from the source to destination and the destination sends the acknowledgement back to the source. During the transmission of message and reception of acknowledgement there is a chance of misbehaviour occurrence among the nodes in the network and the packet mode will be changed to the C-ACK mode and C-ACK packet is sent for detecting malicious nodes. For example, in EEACK mode, source node S first sends an EEACK data packet PACKET1 to the destination node D. If all the intermediate nodes between the Source S to destination D are cooperative then D receives the packet PACKET1 safely, node D is supposed to send the acknowledgement EEACK to node S via the same route but in a reverse order. Within the predefined time period, if node S receives EEACK, then the packet transmission is successful. Otherwise the node S will switch to C-ACK mode by sending a C-ACK data packet to detect the misbehaving nodes in the route.

B. *C-ACK*

C-ACK [7][1]is improvised version of TWOACK scheme. In this scheme every three consecutive nodes work in a group to detect misbehaving nodes. Among the three consecutive nodes the third node should send the C-ACK acknowledgement to the first node. The main aim of the C-ACK is to detect the misbehaving nodes in the presence of receiver collisions or limited transmission power. As in fig.7 Node A first sends C-ACK data packet PACKET1(C) to node B. Then node B forwards this packet to node C. When node C receives PACKET1(C), as it is the third node in this three- node group, the node C is required to send back an C-ACK acknowledgement packet ACK(C) to node B. Node B forwards the packet ACK(C) back to node A. If node A does not receive this acknowledgement packet within a predefined time period, both nodes B and C are reported as malicious. Misbehaviour report will be generated and sent to the source node S. Instead of trusting the misbehaviour report immediately as it happens in TWOACK, in IACK the source node to switches to the MRA mode and confirms this misbehaviour report. This is the main step to detect the false misbehaviour report in the IACK scheme.

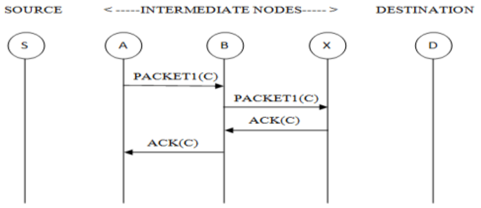

Fig 7. C-ACK

C. *MRA*

MRA [1] scheme is designed to overcome the weakness of the watchdog because it fails to detect the misbehaving node in the presence of the false misbehaviour report. The false misbehaviour report can be generated by the malicious nodes to falsely report the innocent nodes as malicious. This can be lethal to the entire network when the attackers break down sufficient nodes and can cause the network division. 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 in the local network and then seeks for an alternative route to the destination node. If there is no other route, the source node starts a DSR routing request to find another route. By adopting an alternative route to the destination, we can bypass 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.

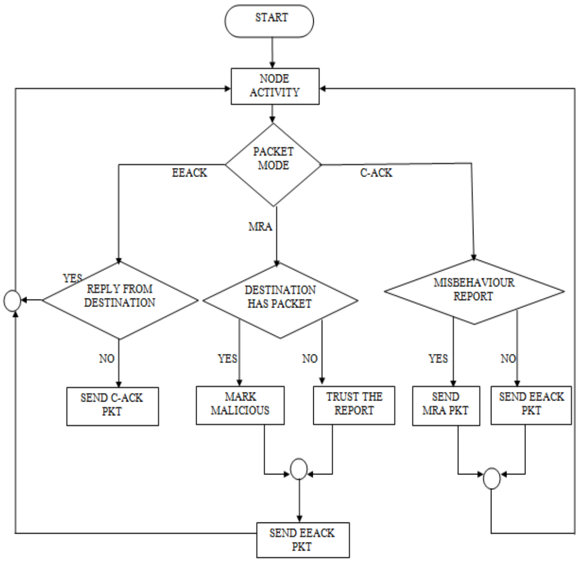

Fig 8. IACK scheme

D. *SCHNORR SIGNATURE*

The schnorr signature is produced using the schnorr signature algorithm[12].The signature scheme is constructed by applying Fiat-Shamir Transform, this can be attached to the data packets for the verification purpose.

CONCLUSION

Eavesdropping and packet dropping is the major threat that is affecting the security in the MANETs. In this paper we have proposed a new IDS IACK protocol specially designed for MANETs.

The proposed scheme can be extended for future work by including the schnorr signature technique during the transmission of the data packets.

REFERENCES

[1] Elhadi M.Shakshuki,Nan Kang and T.R.Sheltami, “EAACK—A Secure IDS for MANETs”,IEEE Industrial Electronics,vol 60,no. 3,March 2013.

[2] A.Tabesh and L.G.Frechette,“A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator”,IEEE Transaction on Industrial Electronic,vol. 57,no.3,pp. 840-849,March 2010.

[3] L.Buttyan and J.P.Hubaux, “Security and Cooperation in WN”,Cambridge University Press,Aug 2007.

[4] L.Zhou and Z.Haas, “Securing adhoc networks”,IEEE netw.,vol. 13,no. 6,pp. 24-30,Nov/Dec 1999.

[5] K.AlAgha,M.-.Bertin,T.Dang,A.Guitton,P.Minet,T.Val and J.-B.Viollet, “Which wireless technology for industrial wireless sensor networks?The development of OCARI technol,” IEEE Transaction on Industrial Electronics ,Vol-56,pp-4266 to 4278,October 2009.

[6] T.Anantvalee and J.Wu, “A Survey on intrusion detection in mobile ad-hoc networks,”in Wireless/Mobile security.NewYork:Springer-Verlag,2008.

[7] K.Liu,J.Deng,P.K.Varshney and K.Balakrishnan, “An Acknowledgement-based approach for the detection of routing misbehaviour in MANETs”,IEEE Transactions in Mobile Computing,vol.6,no.5,pp.536-550,May 2007.

[8] D.Johnson and D.Maltz, “Dynamic Source Routing in ad-hoc wireless networks,”in Mobile computing.Norwell,MA:Kluwer, ch.5,pp.153 to 181,1996.

[9] Basagni.S.,Conti,M.,Giordani S., and Stojmenovic,I.(Eds.), “Adhoc Networking”,IEEE Press Wiley,NewYork,2003.

[10] Abolhasan,M.,Wysocki,T.,and Dutkiewicz,E., “A review of routing protocols for MANETs”,pp. 1-22,Feb 2004.

[11] Royer.E., and Toh.C., “A review of current routing protocols in MANETs”,IEEE Personal comm.,pp.46-55,April 1999.

[12] R.Rivest,A.Shamir and L.Adleman, “A method for obtaining public key crypto systems”,Comm. ACM vol. 21,no. 2,pp. 120-126,Feb 2000.

[13] N.Nasser and Y.Chen, “Enhanced intrusion detection systems for discovering malicious nodes in MANET,”IEEE Int. Conf. Commun.,Glasgow,Scotland,pp1154-1159,June 24-28,2007.

[14] 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.225-265.

[15] G.Jayakumar and G.Gopinath, “Ad hoc wireless networks routing protocol—A review,” J.Comput. Sci.,vol. 3,no. 8,pp. 574-582,2007.