ISSN 2348 – 7968

EAACK—A Secure Intrusion-Detection System for MANETs

Miss. Kalyani S. Ghodake, Miss. Madhura J. Bade, Miss. Poonam A. Pange, Mr. Amit D. Bansode

Department of Computer, Savitribai Phule University of Pune,
Pune, Maharashtra, India

Abstract

The change in networking that is from wired network to wireless network has been a global trend in past few years. The migrating and scalability brought by wireless network made it is easier in many applications .Among all the wireless network mobile-ad-hoc network (MANET) is one of the efficient and unique applications. On the other side of traditional network architecture MANET doesn't require limited network area ; here In MANET Every single mobile node works as both transmitter and reciver.They both communicate with each other directly when they both are within same communication range and area. Otherwise they depend on their neighbor to deliver the message. So this self configuring property of nodes in MANET made it popular among all the wireless network applications like military or emergency recovery.

Keywords: *MANET,* *digital signature, scalability, EAACK, digital signature algorithm.*

1. Introduction

In networking for communication we uses two type of networks .first is Wired and another is Wireless network .because of the mobility and scalability Wireless network is always a first choice .here we are using MANET (mobile ad hoc network).MANET is nothing but the collection of mobile nodes which equipped both the wireless transmitter and a receiver which can communicate bidirectional over the network either directly or indirectly.

MANET creates a temporary network which consist of wireless mobile nodes that creates this network .this temporary network don't have any fixed infrastructure or any central administration .this communication is limited to this transmission range .nodes which are outside from this transmission range that can communicate with each other by intermediate node. The MANET is divided into two types first is single hope .In the singlehop every node has the same transmission range and another type is multihop .In this type every node can communicate with each other by using intermediate node .Without the help of centralized administration MANET is capable for creating self configurable and self maintaining network .Because of this unique characteristics MANET is becoming the more and more widely implemented network in this industry .In this MANET we are using rounting protocols. This routing protocols are generally necessary for maintain effective communication between the distinct nodes.

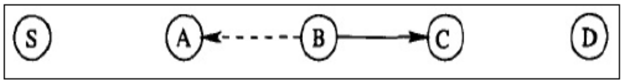
MANET does not contain any fixed infrastructure because of this reason securing wireless ad hoc network is highly challenging issue. This attack can be classified as Denial of service attack, black hole attack, grey hole attack, man –in-middle attack, wormhole attack.

2. Background

Major headings are to be column centered in a bold font without underline. They need be numbered. "2. Headings and Footnotes" at the top of this paragraph is a major heading.

2.1 Watchdog

Watchdog is one of the intrusion detection techniques for MANETs. It improves throughput of network with the presence of malicious nodes. Its aim is to detect malicious nodes misbehaviors in the network. Watchdog finds the malicious activity by listening its next node's transmission. To keep the record of malicious node it has its own failure counter which gets increase when watchdog finds that its next node fails to transmit the data within given amount of time. And when failure counter of given node meets its maximum capacity point then watchdog reports it as malicious node.

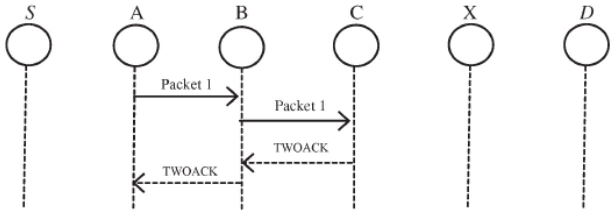


Disadvantages of Watchdog scheme:

- Ambiguous collision
- Receiver collision
- Limited transmission power
- False misbehavior report
- Collusion
- Partial dropping

2.2 TWOACK

TWOACK is not the next version or watchdog based scheme. It is mainly made to avoid the problems of receiver collision and limited transmission power problem of watchdog scheme. To detect the misbehavior of nodes by acknowledging every data packet sent over each three consecutive nodes along the path from source to destination. After receiving data packet, every node needs to send acknowledgment packet to the node which is two nodes away from it.

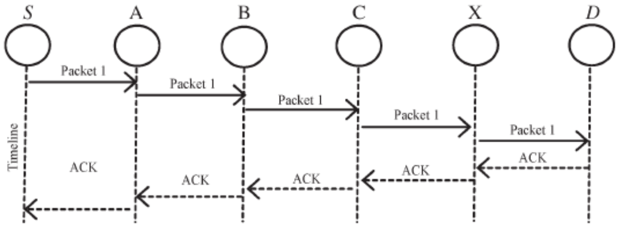


Disadvantages of TWOACK:

- Adds some amount of unwanted network overhead.

2.3 AACK

AACK can also be called as next version of TWOACK. It a combination of ACK (similar to TWOACK) and an end-to-end acknowledgment scheme known as AACK. It efficiently decreases network overhead while it also keeps network throughput and maintenance stable.



2.4 Digital Signature:

In EAACK all its detection schemes depends upon acknowledgment packet to detect malicious nodes in the network. So this causes every package to be verified and untainted. And if the attacker is smart enough to forge acknowledgment packets, then all these schemes are useless. For this very reason we are adopting digital signature in our proposed system. In order to keep integrity of IDS and EEACK we will need all acknowledgment packets to be signed digitally before they are sent out and verified till they are accepted.

Algorithm used:
$s= k^{-1} (H (m)+ xr) \bmod q$
Thus

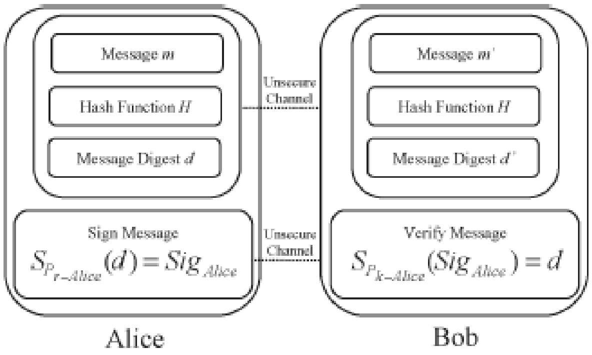
$k= H (m)s^{-1} + xrs^{-1}$
$= H (m)w + xrw \pmod q$

Since g has order q (mod p) we have

$g^k= g^{H(m)w}\ g^{xrw}$
$= g^{H(m)w}\ y^{rw}$
$= g^{u1}\ y^{u2} \pmod p$

Finally, the correctness of DSA follows from

$r= (g^k \bmod p) \bmod q$
$= (g^{u1}\ y^{u2} \bmod p) \bmod q$
$= v$



4. Problem Definition

4.1 ACK

The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet so ACK is end to end acknowledgement scheme. ACK mainly use in Networking to find out misbehaving node in the route for reducing the network overhead and when it unsuccessful then node will switch to S-ACK mode by sending the S-ACK data packet

4.2 S-ACK

In S-ACK three node are work in one group to find out misbehavior node in the network. It is better version than TWOACK scheme because it is detect misbehaving nodes in the presence of receiver collision or limited transmission power. That three node which is work in one route the third node is required to send an S-ACK packet to the first node.

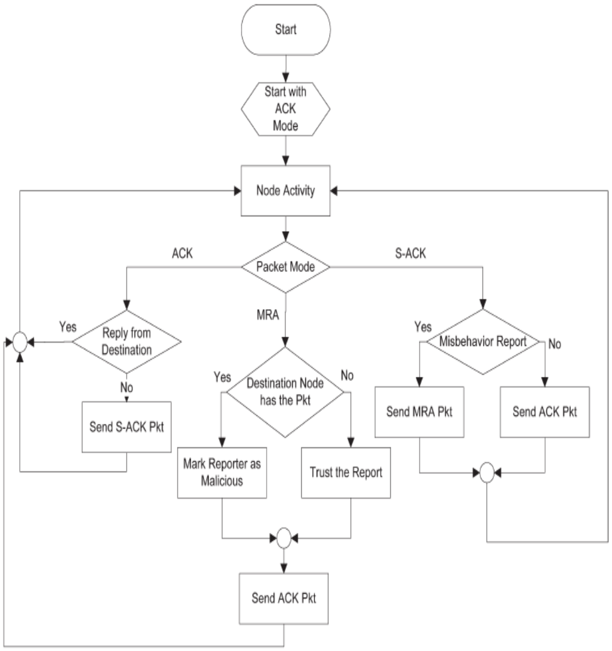
4.3 MRA:

In Misbehavior Report Authentication scheme is to authenticate where the destination node is receive the reported packet through different route. In the MANET when any node give alternative route to the destination node, the misbehavior reporter node .When the destination node gives MRA packet then it searches its local knowledge and compare the reported packet. If it is already receive then understood that this is false misbehavior report and this mark as malicious. Otherwise this misbehavior report is trusted and accepted**.**

4.4 Digital Signature:

EAACK technique is based on acknowledgement so it is very necessary to that all acknowledgment packets in EAACK are authentic. When in MANET EAACK require all acknowledgement packet is digitally signature before they sent out then we can ensure the integrity of IDS.

5. System Architecture:



6. Performance evaluation:

6.1. Simulation configuration:

5.1.1. Packet delivery ratio:

It is defined by the ratio of number of the packets received by the destination node to the number of the packets sent by the source mobile node.

5.1.2. Throughtput:

It can be defined as the average rate of successfully delivered packets over the communication channel. The malicious node sends the false misbehavior report to the source node where it can be possible.

5.1.3. Average end to end delay (AED):

This is used for the average end to end delay to all successfully received packets at the destination node. It can be calculated for each data packet is subtracting the sending time of the packet from the received time at the final destination

7. Acknowledgments

In this paper we have propose the terminologies in security of MANET using EAACK , so we have secured the attacks like Man in the Middle, DOS attacks, Black Hole Attack, Gray Hole Attack. The result of our performance is positive over the traditional secure systems like Watchdog, TWOACK, AACK in IDS which are having negative results in case of receiver collision, limited transmission power and false misbehavior report.

8.References

[1] K. Al Agha, M.-H. 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 Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Net- work Security,” in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[3] 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.

[4] T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in Wireless/Mobile Security. New York: Springer- Verlag, 2008.

[5] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

Second Author biography appears here. Degrees achieved followed by current employment are listed, plus any major academic achievements. Do not specify email address here.

Third Author is a member of the IEEE and the IEEE Computer Society. Do not specify email address here.