Comparative Analysis of Intrusion Detection System Schemes for MANETs

Ruby Dahiya*
Manpreet Singh**
Mohit Jalan***

Abstract

In current information age, the mobile wireless telecommunication becoming more innovative and attractive because of its applications in emerging fields. The attacks has been made from years ago, many schemes were launched to secure data from intruders.

In this paper, comparative study on Intrusion Detection System Schemes for Mobile Ad-hoc Networks has been made. It will present an analysis of performance of the algorithms used for securing data information over mobile network.

Keywords: Watchdog Algorithm, Mobile Ad-hoc Networks, Intrusion Detection Systems, Enhanced Adaptive Acknowledgement

I. Introduction

Intrusion

Intrusion is an unauthorized act of spying, snooping, and stealing information through cyber space. It is defined as a sequence of related actions performed by malicious attacks those results in the compromise of a aim system. It is assumed that the actions of the interloper violate a given security policy.

Intrusion Detection

Intrusion detection (ID) is the technique for identifying and responding to malicious activities targeted at computing and network resources. Intrusion detection is an approach that is complementary with respect to mainstream approaches to security, such as access control and cryptography.

Intrusion Detection System

Intrusion detection systems (IDSs) are software applications dedicated to perceive intrusions against a target network. IDS is placed out-of-band on the network infrastructure, meaning that it is not in the correct real-time communication path between the sender and receiver of information [5].

There are three major modules of IDS: Monitoring, Analyses and Response. The Monitoring Module is responsible for controlling the cluster of data. Analysis Module is responsible for deciding if the collected data indicated is an intrusion or not. Response Module is responsible for managing and using the response actions to the intrusion [5].

IDS in MANETs

A MANET is a mobile ad-hoc network that can change its locations and configure itself on the fly. It uses wireless connections to connect to diverse networks.

The limitation of MANETs is that its routing protocols and nodes assume that other nodes forever help with each other to transmit the data. The assumption leaves the attackers with the opportunities to achieve their target. To address this problem, IDS should be added to enhance the security level of MANETs [2].

Security issues in MANETs

1) MANET is highly vulnerable to attacks because node configuration and maintenance are done on their own [3].

2) One of the primary concerns related to ad hoc networks is to provide a secure communication among mobile nodes in a hostile environment [3].

Ruby Dahiya*
Department of IT
Institute of Information Technology & Management

Manpreet Singh**
Student, IITM
Institute of Information Technology & Management

Mohit Jalan***
Student, IITM
Institute of Information Technology & Management

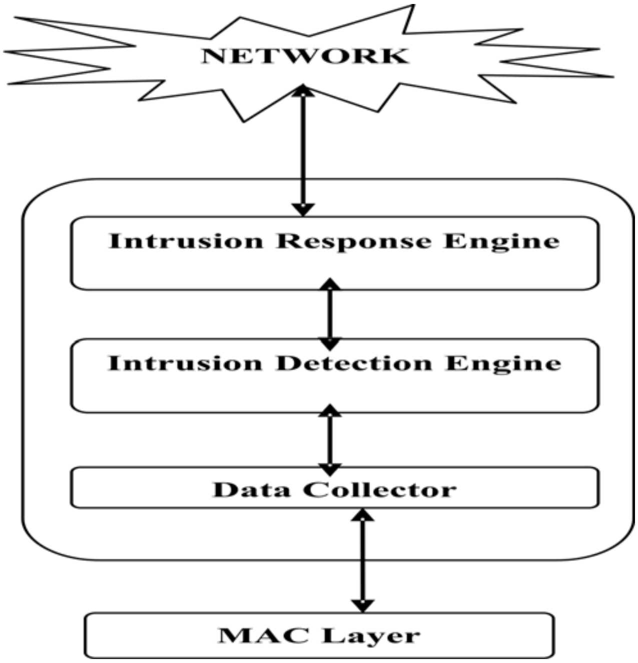

Fig. 1: Intrusion Detection System Architecture for MANETs

3) The ad hoc networks can be reached very easily by users, but also by malicious attackers. If a malicious invader reaches the network, the attacker can easily exploit or possibly even disable the mobile ad hoc network.

In the next section, we will concentrate on the IDS Architecture for MANETs required for understanding this research topic.

II. IDS Architecture For Manets

In fig.1, MAC Layer is the data link layer from where the data packets are send one by one from sender to receiver by means of transmission techniques. To protect the data from intruders, IDS Layer is made in between to secure data.

The Local IDS Agent collects the data from the MAC Layer and sends it to Intrusion Detection Engine for analyzing and processing. The data is further sent to Intrusion Response Engine to give response to the network layer. In this, intruders will get less chances to track data from both the ends i.e. sender and receiver.

In the next section, we mainly concentrate on discussing the various schemes for IDS in MANETs required for understanding this research topic.

III. Various Schemes of IDS in Manet's

In this paper, we will be comparing four various schemes of intrusion detection system in mobile ad-hoc network security. Those are WATCHDOG, TWOACK, and AACK AND EAACK ALGORITHM.

A. WATCHDOG

A watchdog algorithm was made to cope with the problem of attack named as black hole. In this algorithm, [9] each network node connected to other node works as a spectator (watcher) to the next node connected to it. This continues till it reaches to the router or receiver. The watchdog algorithm defines the time limit to each node in which it checks the data by sending time and storing time. If the sending time is more than the storing time then that node is being marked up as a harmful/mischievous node. If something like this happens then the path rater gets active with routing algorithms and ignores that node in between the transmission [9].

B. TWOACK

This algorithm states that the communication between the dispatcher and the recipient is on the basis of the two hops or we can say the three nodes communication.

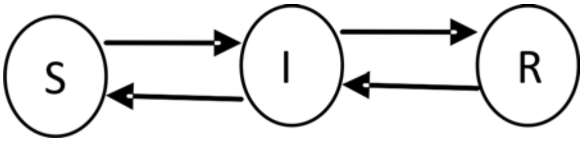

Fig. 2: TWOACK algorithm

Fig.2 states that S is the sender and R is the receiver just two hopes far from S and I is the intermediately knot in between the S and R. [1] So while transmitting the data, S will send the packet to the I (Intermediatory) node and I will send that packet to the R. On completion of this process, R will send back the ACK (Acknowledgement) for the packet to the S. If TWOACK packet doesn't get back to the S in define time period both the nodes I and R are defined as harmful/malicious nodes. This process goes up for all the nodes till destination.

C. AACK

Adaptive ACK ALGORITHM is being termed as end-to-end Acknowledgment. Basically, it is a combination of peer-to-peer Ack and TWOACK.[8] As TWOACK send the acknowledgment packet to the node two hops, in AACK this process is done from the sender to the receiver/destination end.

The S sender or source sends the packet to the R Receiver or Destination by the intermediate nodes i.e. A, B and C. Each node passes the packet to the next node and then get the Acknowledgment in the reverse order to the sending route. If the sender doesn't get the acknowledgement then it sends it by TWOACK algorithm to find the harmful node in between.

D. EAACK

EAACK is being termed as Enhanced Adaptive Acknowledgement. [2] This algorithm is a combination of three things i.e. ACK, SACK and MRA.

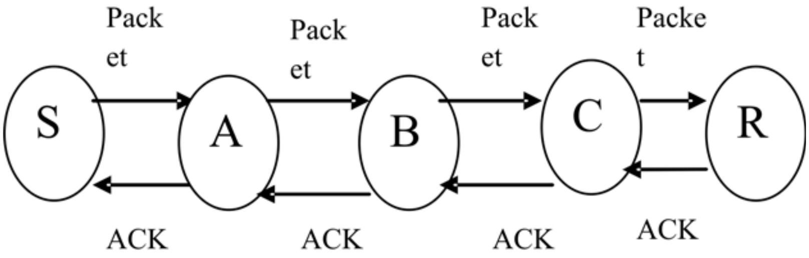

Fig. 3: AACK algorithm

ACK is being used for peer to peer communication when there is no such harmful node in between.

SACK is an advance form of the TWOACK which is used to detect the malicious node or the harmful node.

MRA is an algorithm which is used to search the routing path into its local databases. [5] If the algorithm does not get the path, then sender starts DSR routing algorithm to find another way to transmit the packet to the destination.

In the next section, we will concentrate on comparison of various schemes for IDS in MANETs.

IV. Comparison of Various IDS Schemes in Manets

Here, we have compared four schemes namely: Watchdog, TWOACK, AACK and EAACK for intrusion detection in MANETs. The factors used for their comparative analysis are: Ambiguous Collision, Receiver Collision, Limited Transmission Power, False misconduct report, Collusion, Partial Dropping, Network Overhead and Detection. The Table shown below represents the comparison of IDS Schemes for MANETs.

IV. Conclusion

The Mobile Ad-hoc Network is a new technology used in many applications. Because of its characteristics, the networks are more vulnerable to attacks and have most security problems. In this paper, the comparative analysis is made on IDS schemes for MANETs to explain best suited algorithm.

Table 1: Comparison of Various IDS Schemes in Manets

Factors Schemes	*Ambiguous Collision*	*Receiver Collision*	*Limited Trans-mission Power*	*False Mis-conduct report*	*Collusion Dropping*	*Partial Overhead*	*Network*	*Detection*
Watchdog Algorithm	Yes	Yes	Yes	Yes	Yes	Yes	No	Malicious Nodes
TWOACK Algorithm	Yes	No	No	Yes	Yes	Yes	Yes	Malicious links
AACK Algorithm	Yes	No	No	Yes	Yes	Yes	Yes, but reduced	Malicious Links
EAACK Algorithm	No	No	No	No	No	No	No	Malicious Nodes

The Watchdog algorithm aims to improve the throughput of network in presence of malicious no design in the network. It has no network overhead compared to other schemes of IDS.

The TWOACK Algorithm aims to solve the receiver collision and limited transmission power. The network overhead is more as well as it fails to detect malicious nodes in the network with presence of false misbehavior report and forged acknowledgement packets.

The AACK algorithm combines TWOACK and an end-to-end acknowledgement scheme (ACK). It reduces network overhead compared to other schemes and it fails to detect malicious nodes in the network as TWOACK Scheme.

The EAACK has no network overhead and detects malicious nodes in the network. To prevent attackers from initiating forged acknowledgement attacks, a digital signature is incorporated in the scheme.

References

1. Ehsan Amiri, Hassan Keshavarz, Hossein Heidari, Esmaeil Mohamadi, Hossein Moradzadeh, "Intrusion Detection Systems in MANET: A Review", ICIMTR, Malaysia, 22 – 23 September, 2013
2. Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK- A Secure Intrusion Detection System for MANETs" IEEE trans. vol.60, no.3, March, 2013
3. Nithya Karthika, M Raj Kumar, "Intrusion Detection System Using EAACK and digital signature for authentication in MANET", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 2, March-April, 2014
4. Ms Priyanka P Kulkarni, "A Survey on Secure Intrusion Detection System for MANET", Ijarcsse, Volume 5, Issue 1, January 2015.
5. Ranjit j. Bhosale, Prof. R.K.Ambekar, "A Survey on Intrusion detection System for Mobile Ad-hoc Networks", IJCSIT, vol. 5 (6), 2014, 7330-7333
6. S.Gangwar, "Mobile Ad Hoc Networks: A Comprehensive Study and Survey on Intrusion Detection", (IJERA), vol.2, No.1, pp 607-612, 2012.
7. Satria Mandala, Md. Asri Ngadi, A.Hanan Abdullah, "A Survey on MANET Intrusion Detection", IJCSS, Vol (2): Issue (1)
8. S. Sahu and K. Shandilya, "A Comprehensive Survey on Intrusion Detection in MANET", IJITKM, Vol.2, No. 2, pp. 305-310, 2010.
9. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad-Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.
10. T. Prasanna Venkatesan, P. Rajakumar, A. Pitchaikkannu, "An Effective Intrusion Detection System for MANETs", ICACEA-2014 at IMSEC, GZB.