

A Survey on Intrusion Detection Systems in Mobile Ad-hoc Networks

Sonika H.R.¹, Poornnima B.G.²

PG Scholar, Department of CSE, Vidya Vardhaka College of Engineering, Mysuru, India¹

Associate Professor, Department of CSE, Vidya Vardhaka College of Engineering, Mysuru, India²

Abstract: Now a day the technology is improving day by day. The wired network has been changed to wireless network. There are many advantages of wireless network over wired network. One of the main advantage is we can walk around freely in a network area and accesses internet. Security is one of the challenging issues. Intrusion Detection System is one of the systematic ways to detect malicious node in a mobile ad-hoc network (MANET) and it is driven by battery power. This paper gives a survey on various intrusion detection systems in MANET.

Keywords: mobile ad-hoc network (MANET), Intrusion Detection System (IDS), malicious, security.

I. INTRODUCTION

An intrusion Detection System (IDS) is a software application that detects malicious activity in a network and reports it to the source or administrator.

MANET is a mobile ad-hoc network. It can configure by itself and it can change the location. Because of its mobility they use wireless network.

There are two types of link single hop and multi hop. Single hop is one which there is no link between two nodes. Multi hop is one which there is intermediate node between two nodes.

Security in MANET is important thing in a network. Encryption and authentication can reduce intrusion but it cannot be eradicated. Hence intrusion prevention is first line of defense. Intrusion Detection provides second line of defense.

This paper shows a survey on various intrusion detection systems in Mobile Ad-hoc Networks. Section 2 gives intrusion detection system for Mobile Ad-hoc Networks. Section 3 gives conclusion.

II. INTRUSION DETECTION IN MOBILE AD-HOC NETWORK

Fangchao Yin et al [1] in 2009, concentrated on enhancement of Intrusion Detection System in Mobile Ad-Hoc Network. Its aim is to improve the data analysis and pattern matching algorithm based active set. It presents Intrusion Detection System and General Intrusion Detection Model which has data source module, pattern matching module. The core Intrusion Detection data analysis and pattern matching presents the active set method and improved pattern matching algorithm therefore efficiency of Intrusion Detection can be improved for some extent.

Yinan et al. [2] in 2010, introduces an Agent-based Intrusion Detection System for Mobile Ad-Hoc Network. Cluster is a group of node and the node with highest battery level is treated as cluster head. The Intrusion Detection System in MANET can be divided into three structures (i) isolated Intrusion Detection System every host has Intrusion Detection System and detects attack independently. (ii) Plane Structure every node executes the Intrusion Detection by gathering local data. (iii) Hierarchical Structure separates the whole MANET into multiple Intrusion Detection System (IDS) clusters by cluster; and the Intrusion Detection activity is executed by cluster head. The network extensibility has improved and a little network control overhead which can realize Distributed Intrusion Detection.

Intrusion Detection System Agents run on each node, which consumes more energy for each node. The lifetime of total network, is decreased. The solution for the problem is that taking the cluster head as detection unit based on Agent that is dividing network by proper clustering algorithm and activating Agent System on cluster-head node at the same time. This has an advantage of little route overhead and also has an advantage of saving the system resource and this model has high detection rate and also effectively decrease the false detection rate.

Hajar Al-Hujailan et al. [3] in 2011 proposed a scheme called Cooperative Intrusion Detection Scheme. For basic function of a network such as routing, packet forwarding, network management and so on, security in MANET is very important. The IDS has two main parts they are detection process and response process. Detection process has three agent local detection engine, local data collection and cooperative detection engine. Response process has three agents local response, secure communication, global response. They added one more agent to response process



called “cooperative collection”. The cooperative collection is one which the activities are shared among the nodes to take correct decision against malicious nodes.

In the proposed scheme the data structure needs some tables and packets. There are three types of tables “PACKET_TABLE”, “HEAD_MALICIOUS_TABLE” and “MALICIOUS_TABLE”. There are six types of packets “notification”, “warning”, “Acknowledgement”, “new_request”, “new_info” and “new complete”.

They designed a group of node called cluster and each cluster has a HEAD and assumed that all HEAD are trusted. It works as a response for detection process. Also assumed that attacks at the node needs recovery. The entire cluster HEAD has a recovery process and also have identifier (node_id) and the id cannot be changed even if node leaves the network. This scheme overcomes the attack effectively. It also reduces the false rate without increasing in the overhead.

BapiKisku et al. [4] in 2012, proposed An Energy Efficient Scheduling Scheme for IDS in MANET. Energy and security are two main things in MANET. Due to disaster occurred in energy level of the node the IDS cannot run throughout the life time. The solution is Novel Scheduling strategy is used in which all the IDS will run in the time sharing fashion in a bunch. This will improve the energy level in a cluster. Energy is saved and thus the security in MANET also improved. The scheduling strategy is an impression of game theoretic approach. All the IDS of a group of node based network will be scheduled in a time shared manner.

The scheduling approach does not make impartial in terms of load sharing. After the scheduling scheme, up to 5 percent of crash can be tolerated by IDS. The energy of the node will be saved and security will be increased. Thus average life time of the network will be improved. The message overhead may take place and there may be decrease in network partition.

DrB.Paramasiva et al. [5] in 2013 address a novel Intrusion Detection System which uses game theoretic model to find malicious node at the beginning. The Bayesian game concept of game theory have been used to model the interaction between any two neighboring node of MANET and this results in finding the optimal strategy for regular node and malicious node of the network. The node observes carefully its neighboring node and stores the information about packet sent and received based on game.

Bayesian games are the combination of game theory and probability theory that allows taking the incomplete information. In any circumstances the player are not informed about opponent action. Thus there will be the game of incomplete information of non-cooperative game. Each player has some secrete information that will alter

the progress of game. These beliefs are represented by probability distribution and update previous communication whenever new information is available.

According to this proposed architecture each mobile node in network are responsible for observing, finding attacks and generating alarm to attack detected.

ShivaniUyyala et al. [6] in 2014 proposed an Anomaly based Intrusion Detection of packet dropping attacks in MANET. Packet dropping is one of the harmful attacks in MANET.

The packet dropping attacks has two types a) black hole and b) grey hole. In both case the malicious node sends the false response to the sender that is having shortest route to the destination. In black hole attack, attacker drops the entire packet received from the source node. In grey hole attack the attacker drops some of the packet and forward it and does not send the data packet. The proposed system is to find and isolate black hole and grey hole attack.

Routing protocol can be affected by this packet dropping. The proposed mechanism carefully observes and finds malicious node. Monitoring the node has a function such as the network has a unique id and thus it can be distinguished from other node. Neighboring node can be covered by monitoring node, using this method at network layer monitoring node observes the neighboring node character, when there is malicious node the monitoring node informs all other node in a network. Thus by isolating black hole and grey hole the network performance can be improved.

ElizaethSherine .M [7] in 2015 proposed Effective Intrusion Detection Method for MANET using Enhanced Adaptive Acknowledgement (EAACK). EAACK overcomes the limitations such as watch dog, TWO ACK, AACK. EAACK included three significant part such as ACK, secure ACK(S-ACK), and Misconduct Report Verification (MRA). It is expected that the association between every hub in a system is bidirectional. Both the source and destination hub can be trusted. It uses Dynamic Source Routing to find shortest path to reach the destination. The sender encodes the data with advanced mark and sends to the destination. The receiver decodes the data and check the signature for verification of data.

III. CONCLUSION

Wireless network are more popular then wired network. MANET is a Mobile Ad-Hoc Network with no fixed infrastructure with wireless connection. Security in MANET is critical issue. Prevention of malicious node by authentication and cryptography becomes first line of defense. IDS in MANET are a second line of defense. From the survey we have reviewed different technique and methods for IDS in MANET. We have tried to show difference between the methods used.

**REFERENCES**

- [1] Fangchao Yin, XinFeng, Yonglin Han, Libai He, Huan Wang, "An Improved Intrusion Detection Method in Mobile", 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.
- [2] Yinan Li, ZhihongQian, "Mobile agents-based intrusion detection system for mobile ad hoc networks", 2010 International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering.
- [3] Hajar Al-Hujailan, Mznah Al-Rodhaan, and Abdullah Al-Dhelaan, "A Cooperative Intrusion Detection Scheme for Clustered Mobile Ad Hoc Networks", 2011 7th International Conference on Information Assurance and Security (IAS).
- [4] BapiKisku and Raja Datta, "An Energy Efficient Scheduling Scheme for Intrusion Detection System in Mobile Ad-hoc Networks", 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.
- [5] Dr. B. Paramasiva, K. MohaideenPitchai, "Modeling Intrusion Detection in Mobile Ad Hoc Networks as a Non Cooperative GAME", Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22.
- [6] ShivaniUyyala, DineshNaik, "Anomaly based Intrusion detection of Packet Dropping Attacks in Mobile Ad-hoc Networks", 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) .
- [7] Elizabeth Sherine.M, "EFFECTIVE INTRUSION DETECTION METHOD FOR MANETs USING EAACK" 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT].