Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 50 (2015) 109 – 114

Procedia
Computer Science

2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

# Fuzzy Based Intrusion Detection Systems in MANET

Vishnu Balan E, Priyan M K, Gokulnath C, Prof.Usha Devi G

*School of Information and Technology, VIT University - Vellore Campus, Tamilnadu, India*

*E-mail: vishnubalan91@gmail.com, priyanit085@gmail.com, gokulkapoor@gmail.com, ushadevi.g@vit.ac.in*

**Abstract**

Mobile adhoc network (MANET) is an infrastructure less wireless network and self-organized. During communication mobile adhoc network do not use any proper infrastructure so that MANET initiates request for data transfer, so MANET is vulnerable to various type of attacks such as black hole attack, warm hole attack, gray hole attack. The proposed system is to detect the malicious behavior of node by intrusion detection system with fuzzy logic technique and also to identify the type of attacks. The system is robust enough to detect attacks such as black hole attack and gray hole attack and also able to prevent those kind of attacks by using efficient node blocking mechanism such that the proposed system provides a secure communication between nodes

*Keywords:* mobile adhoc network (MANET);fuzzy logic technique;black hole attack;gray hole attack;

## 1 INTRODUCTION

In recent years, mobile adhoc networks (MANET) are flexible to various types of application because of its flexibility. There is no fixed infrastructure for MANET, so this facility makes mobile adhoc networks very effective for military application. Each node requests nearby node by using various routing protocols such as AODV, DSR and OLSR to transfer data from one node to another node. But MANET is vulnerable to various types of attacks because of its feature such as communication via wireless links, resource constraints, and dynamic topology.

Many intrusion detection system (IDS) have been developed for MANET to detect various types of attacks, IDS plays crucial role in MANET to detect any type of attacks. An IDS is a software system that is used to analyse misbehaviour and violation of policy, then generate report based on this. Basically intrusion detection system is classified into three types, they are signature based detection, anomaly based detection and specification based detection. The signature based detection compares the signature of existing patterns with network pattern, if any existing attack pattern matches with network pattern then the network is attacked. The anomaly detection is further classified into statistical based, knowledge based and learning based. The anomaly detection considers the normal behavior of networks and also flag the unknown activity, based on this it generates alarm.

## 2 LITERATURE SURVEY

Recent research in MANET is to detect and prevent the specific attack in the network. Kurosawa and Jamalipour (2007) proposed a mechanism for black hole detection for AODV. Fuzzy based genetic algorithm has been proposed by Wang Yunwu (2009) which uses initial rules from fuzzy algorithm and final rules from genetic algorithm. Genetic based intrusion detection system for TCP/IP networks has been proposed by Wei li (2010).Yi et al (2005) considered RREQ flooding attack, so they invented a new mechanism to prevent RREQ flooding attacks based on the next node supervision. Hu et al (2003) experimented how an attacker can use a rushing attack in the network in DSR and implemented a new method for rushin attack prevention mechanism for MANET. Though many analysts were trying to prevent the network from the attack, some researchers were suggested with general approach. Jungwan Kim et al (2001) proposed the artificial immune system for IDS and it is based on hierarchical approach which is inspired by human immune system. A same approach, Ariadne has proposed a mechanism for end-to-end delivery based on the key that has been shared. More effort is needed to prevent the network from attack. Mechanism proposed in above method is to protect network against other attacker through routing.

doi:10.1016/j.procs.2015.04.071

The intelligent based intrusion detection systems is used I network to find the intruder node using attributes. Similarly IAWDO and IAMSV method were proposed to detect the intruder in distributed environment that use of trust in transactions. Energy Based Trust Solution System finds a node whether it's an intruder's node or not depending on the trusties has four components to find the intruder node. They are 1. Supervisor module 2. Aggregator module 3. Trust calculator module and 4.Disseminator module. The supervisor module will supervise the next node using Passive acknowledgement (PACK). PACK is used to detect whether nodes are forwarded to correct node or not, by supervising their communications. Based on the communication, if there is any difference in the nodes then the aggregator component does it work.

## 3 PROPOSED METHOD

The proposed system consists of three main blocks: they are attack categorization, fuzzy implementation and fuzzy estimation.

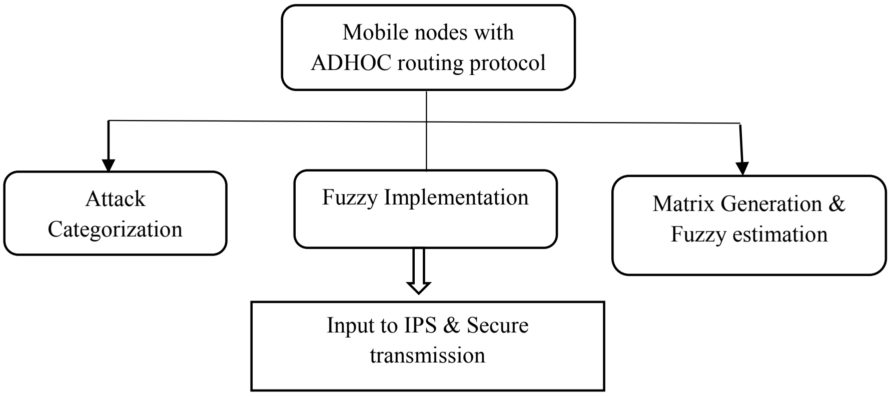
Mobile nodes with ADHOC routing protocol
Attack Categorization
Fuzzy Implementation
Matrix Generation & Fuzzy estimation
Input to IPS & Secure transmission

Figure 1 System Architecture

### 3.1 Attack categorization

The MANET attacks are broadly classified into two types [Revathi et al, 2012], they are external attacks and internal attacks. The internal attack is performed by compromised node belongs to the same network. The external routing is initiated by outside source which replay false routing information or old routing information to increase the network overload. The proposed system mainly suitable for two attacks such as black hole attack and gray hole attack

### 3.1.1 Gray hole attack

This attack leads to dropping of packets. The attacking node initially behaves correctly and reply correct route reply message to node which initiates the RREQ message. Afterwards the node fails to forward the packet which leads to dropping of packets, then the network get damage. In any case the node always try to find exact route information which makes the particular node to consume more energy and therefore this attack leads to dropping of packets and consume its battery more. If the gray hole present near source node then it is gray hole towards source and similarly if the gray hole present near the destination then it is gray hole towards destination.

### 3.1.2 Black hole attack

Black hole is similar to gray hole attack but in black hole attack the malicious node never send the initial route message correctly as like in gray hole attack, rather it waits for neighbour RREQ message. If the attacker node receives the RREQ message from neighbour then it sends false routing RREP with highest sequence number to neighbour node before the correct RREP reach the neighbour. So the neighbour thought the false RREP is the correct one and send the message by using the false information. So the data packet never reaches the destination properly. Similarly the attacker node attacks all RREQ messages. To succeed in this attack the malicious node should present in the centre of the network.

Gray hole attack one or two nodes to isolate the network whereas the black hole attack affects the entire network. This module categorizes the type of attack and sends information to next fuzzy implementation module.

### 3.2 Fuzzy implementation module

Fuzzy logic uses various measures of number of packets dropped against various parameters. The fuzzy techniques overcome the problem which was not solved by existing techniques. The fuzzy logic technique is very easy to implement and produce precise output by removing various ambiguities. Since three attacks are used in this paper, three measures are used to calculate fuzzy