

Intrusion Detection System for Secure Data Transmission in Mobile Ad hoc Network

Vijayakumar.P^{#1}, Tamizharasan.P^{*2}

¹M.Tech, Department of IT,
¹vijay248kumar@gmail.com

²Assistant Professor, Department of IT,
²tamizh.mtech@gmail.com

^{1,2}V.S.B Engineering College,
Karur, Tamilnadu, India.

Abstract - Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. MANET has been normally deployed in network for forwarding the data from one node to another. To avoid the routing attacks MANET has been deployed in the network. In previous solutions typically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. Every node in MANET plays a router role while transmitting data over the network. While transmitting the data over the network the Whole file can be divided into different packets. For each packet the key value will be assigned and send to intermediate nodes. Attacks can be further categorized as either outsider or insider attacks in MANET routing. With routing packet attacks, attackers could not only prevent existing paths from being used and also spoof non existing paths to lure data packets to them which have been carried out on modeling MANET routing attacks using routing table recovery. This routing table recovery intimates intrusion response to the client.

Keywords—Mobile Adhoc Network, Dempster Shafer Theory, Naive Fuzzy

I. INTRODUCTION

Mobile ad hoc network (MANET) is a new emerging technology which enables users to communicate without using any fixed or physical infrastructure. Ad-hoc network, as its name indicates is a collection of nodes that are connected arbitrarily for some temporary time without the aid of any fixed infrastructure. In a MANET, nodes can freely move around while communicating with each other. These networks may under-perform in the presence of nodes with a selfish behavior, particularly when operating under energy constraints. Nodes that lie within each other's send range can communicate directly and are responsible for dynamically discovering each other.

In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The success of communication highly depends on other nodes cooperation. Therefore, MANET has the property of rapid infrastructure-less deployment and no centralized controller which makes it convenient to many environments, such as battlefield, emergency disaster relief and business meeting. Due to inherent characteristics of MANETs, it is subject to different

vulnerabilities. Also most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious. Prevention approaches such as cryptography and authentication were proposed to and implemented. However, such prevention methods alone are not sufficient to make them secure therefore, detection should be added as another defense before an attacker can hack the system. Once an IDS detects an abnormal activity it generates alarm or initiate a response to the corresponding malicious activity.

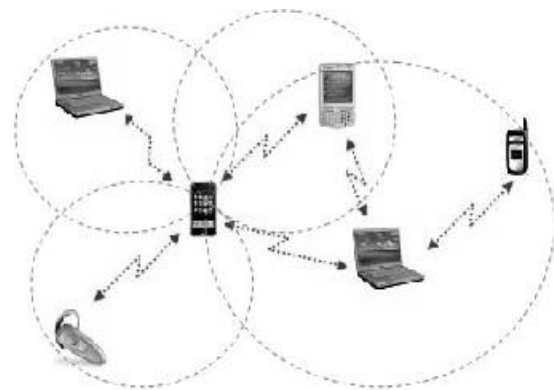


Fig. MANET Infrastructure

Generally Intrusion detection can be classified based on the collected audit data as either host based or network based. A network-based IDS captures and analyzes packets from network traffic and a host-based IDS uses application logs for its analysis. Based on detection techniques, IDS can also be classified into the following categories

- **Anomaly detection:** Here the normal behaviors of users are compared with the captured data, and then treats any activity that deviates from the baseline as a possible intrusion. Then this information is passed to the system administrator.
- **Misuse detection:** The system keeps patterns of known attacks and compares these patterns with the captured data. Any matched pattern is treated as an intrusion. Then the proper response is initiated.
- **Specification-based detection:** In this detection method the system defines a set of constraints that describe the correct operation of a program or protocol. Intrusion is identified based

the violations of these constraints. Several intrusion detection techniques were developed for wired networks. But they were not suitable for MANETS due to its different characteristics. New approaches need to be developed or else existing approaches need to be modified for MANETS. In literature, several intrusion detection systems of MANET are developed using machine learning techniques. Some IDS uses single learning technique such as neural networks, fuzzy logic and support vector machines etc. On the other hand, some IDS use the combination of two or more techniques. Lot of reviews have been made on IDS of MANET. However, there is no a review of machine learning techniques over the intrusion detection domain of MANET. This paper presents a comprehensive analysis and evaluation of the most recent literature in the area of machine learning techniques in intrusion detection for MANETS. The rest of the paper is organized as follows.

This paper explains the secure data transmission through the router without any malicious attacks. If having any malicious nodes it intimate and perform action.

II. ARCHITECTURE DIAGRAM

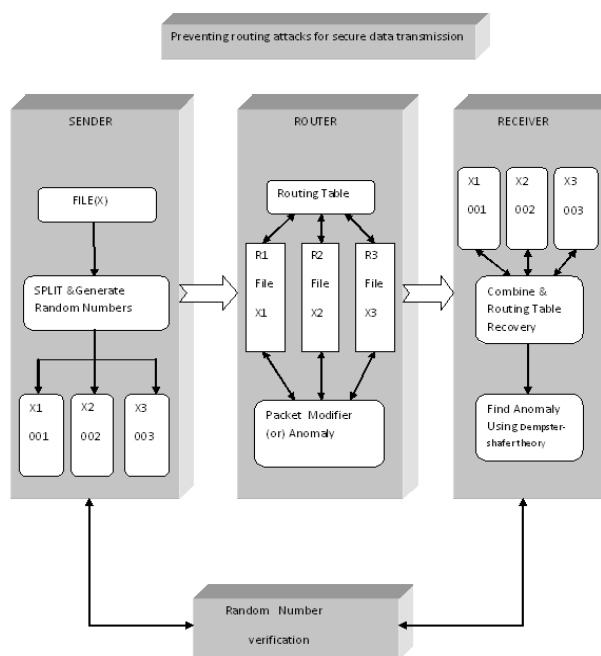


Fig. Architecture Diagram

- In sender system the file can splitted into number of files using file splitting algorithm
- The sender will assign the key values for each file and send to Intermediate router IP. The Key value will be generated by using key generation algorithm.
- The Packets will receive from different intermediate router in client system. If the intruder is changing the file, the key value will be changed in the routing table. The intermediate router who will change file that router will be a hacker.

- The modified file packets will send to receiver. The receiver will join the file by using packet marking id and Key value. The Routing table has the different routing values for the corresponding packets from the different intermediate router IP.
- In receiver that is client system will Compare the Routing table values with the Packet marking values, If both the values are matches, the client can download the Original file else they can find the hackers.

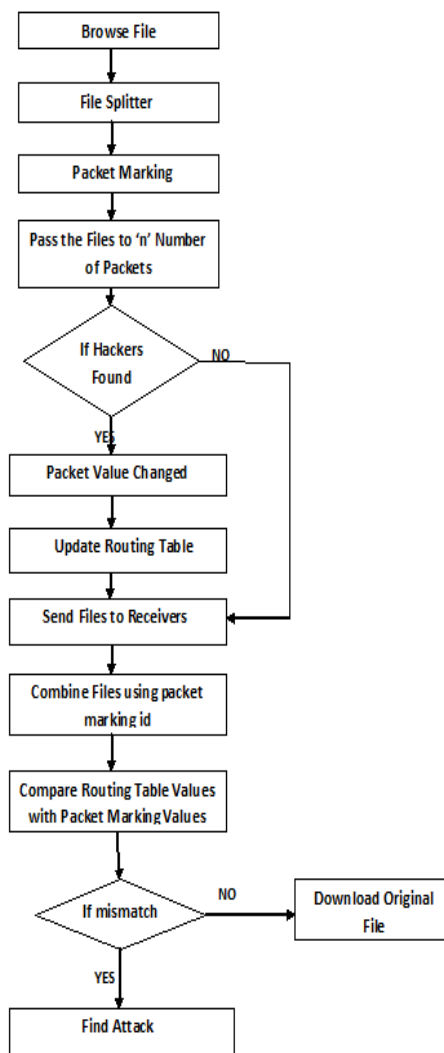


Fig. System Flow Diagram

Client send request to the server for access, if the server permission user send file via router. User split the file using the file splitting algorithm and send to router1.in the server hacking mode off mean hacker cannot access router the file automatically received to destination. If hacker access router mean server will generate security key with the help of key generation algorithm. After creation of security key hacker cannot access router then file received to receiver system.

Data Flow Diagram

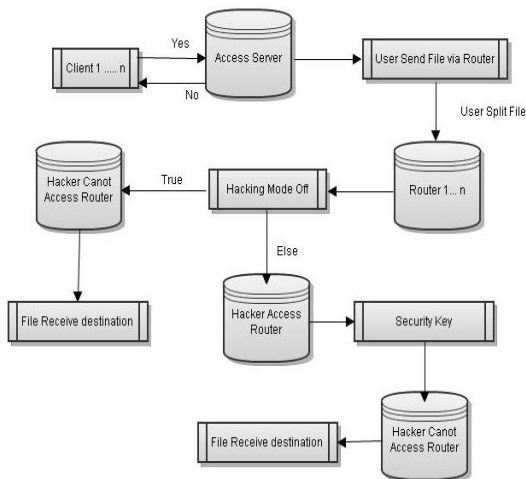


Fig. Over all DFD Diagram

III. SYSTEM MODULES

This paper explains the secure data transmission between the client and server through the router without any malicious attacks. If having any malicious nodes it will inform to the client. In this paper contains the following modules

- Client request
- Server response
- Intruder risk
- Decision making

Client Request

In this module explains the client request to the server system. It contains the all request and their IP address to the server. Client system will merge all the file from the router. In this key value real number means it does not affect by intruder, the value is null means that file affected by intruder in intermediate router.

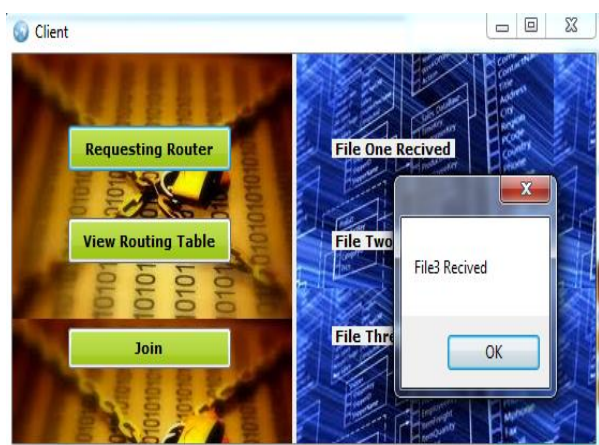


Fig. Client System Receives Files

Server Response Module

This contains the server side system. Here the file will be select for sending to client. This file contains the large size means it will splitted into three parts using file split algorithm and send to intermediate router. For sending this file, path will find using protocols and choose the client IP address.

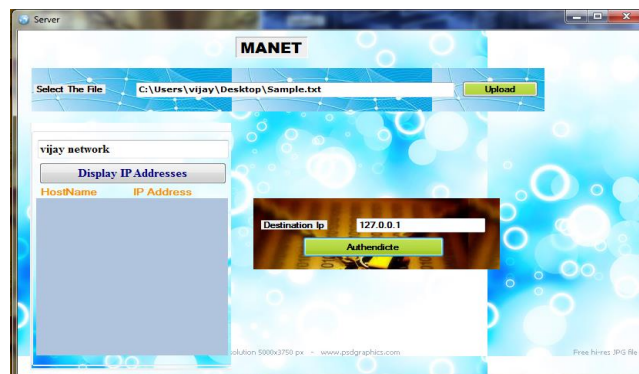


Fig. File Selection in Server

Intruder Risk

It contains the intrusion detection of hacker. Here the file is send via three different routers. Router, router1, router are router which will send splitted file from server. In this router two types of option available hacker mode on and hacker mode off. If the hacker mode off means the original file will send to client or the hacker mode on means hacked file that is modified file will send to client.

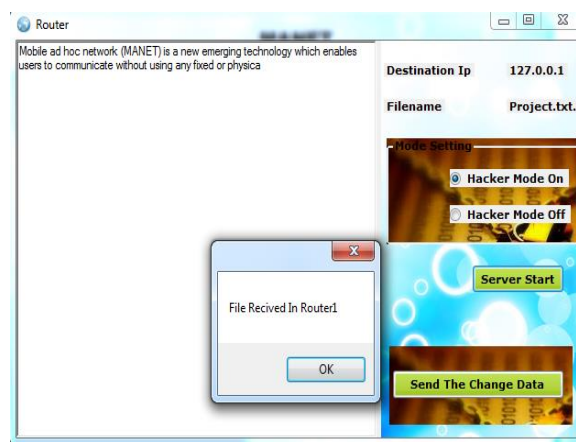


Fig. Intermediate Node Receive the Data

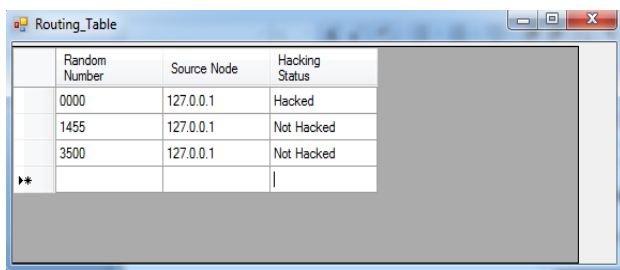
Decision Making

Routing Table

The client contains the three types of option.

- Client Request
- Routing Table
- Joins

Routing table used to display the files received from router with the random number value, source node IP address and status of hacking. In this random value null means that file hacked by intruder, the random value not null means the file not hacked by intruder. The hacking status shows which part of file hacked or not hacked.



Random Number	Source Node	Hacking Status
0000	127.0.0.1	Hacked
1455	127.0.0.1	Not Hacked
3500	127.0.0.1	Not Hacked

Fig. Routing Table Values

IV. CONCLUSION

In this paper we have propose a system for intrusion detection in MANET using proactive protocols. In this system detect both the malicious node and hacker by using intrusion detection system, with the help of this system the secure true data to be transmitted from server to client via the routers. This system will reduce the time because the file to be split and send to client. With the help of random value we can easily find the hacker node or malicious node.

REFERENCES

- [1] Rusha Nandy, Debduitta Barman Roy” Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme” Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011).
- [2] Ziming Zhao, Gail-Joon Ahn, “Risk-Aware Mitigation for MANET Routing Attacks”, IEEE transactions on dependable and secure computing 2012
- [3] Kartik Kumar Srivastava, Avinash Tripathi”, Secure Data Transmission in MANET Routing Protocol”,Int.J.Computer Technology & Applications,Vol 3 (6), 1915-1921.
- [4] PriyankaGoyal, Vinti Parmar,Rahul Rishi” MANET: Vulnerabilities,Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011
- [5] Lili Sun, Rajendra P. Srivastava,” An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions”.

- [6] Yan Lindsay Sun, Zhu Han,” Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks”, IEEE journal on selected areas in communications, vol. 24, no. 2, february 2006.
- [7] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc on-demand distance vector routing,” Mobile Ad-hoc Network Working Group,vol. 3561, 2003.
- [8] Amit Shrivastava, Aravinth Raj Shanmogavel,”Overview of Routing Protocols in MANET’s and Enhancements in Reactive Protocols”.

AUTHORS PROFILE



Mr.P.Vijayakumar Pursing the M.Tech (IT) in V.S.B Engineering College. He has received B.E (CSE) degree from Angel College of Engineering and Technology. He has total number of 7 publications, 2 paper in International journal , 2 papers in International conferences and 3 papers in National conference participated in various symposiums and workshops held at different places. His area of interest includes Wireless Network Mobile computing and Data Structures.



Mr.P.Tamizharasan has received the B.Tech (IT) degree from Anna University and M.Tech (IT) degree from Dr M.G.R Educational and Research Institute. He is currently working as an assistant professor in V.S.B Engineering College. His area of interest includes Network Security, Data Mining and Steganography, MANET.