Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 91 (2016) 38527-38530

ISSN: 2229-712X

An Effective Intrusion Detection System for correction and detection of Gray Hole attack in MANETs

Shivani Sharma and Tanu Preet Singh

Department of Computer Science & Engineering Amritsar College of Engineering & Technology, Amritsar, India.

ARTICLE INFO

Article history:

Received: 20 March 2013;

Received in revised form:

18 February 2016;

Accepted: 23 February 2016;

Keywords

MANETs,

Grey hole attack,

IDS.

ABSTRACT

Mobile Adhoc Networks is a collection of wireless mobile nodes, which form temporary networks without relying on any existing infrastructure or centralized administration or standard support services regularly available in wide area networks to which the host may normally be connected. In this paper the simulation results has been compared between previous & current approach for the correction and detection of Gray Hole attack in MANETs and all the results are taken by NS2 Simulator.

Introduction

The term Adhoc Networks dates to the 1970 were an Adhoc Network was first step as a part of certain difference research projects with advances in micro electronics technology and networking protocols. It has been possible to integrate mobile notes and various other network devices into a single unit called an Adhoc node [12]. Adhoc is a Latin word which means "for this only". Mobile Adhoc Network is an autonomous system of mobile nodes connecting by wireless links. Each node operates as an end-system and a router for all other nodes in the network [10]. A MANETs is formed by an autonomous system of mobile nodes that are self-configuring and have no constrains, such as a fixed infrastructure or a central administration system. Nodes in MANETs are both routers and terminals. They are dynamic in the sense that each node is free to join and leave the network in a deterministic way[12]. They do not have defined feasible boundary and any specific entry or exit point.

Characteristics of MANETs [10]

1. Network is not depending on any fixed infrastructure for its operation.
2. Ease of deployment
3. Speed of deployment
4. Each node is working as intelligent node.

Adhoc Applications [10]

1. Tactical Networks: Military communication automated system.
2. Entertainment: Multi user's games, Robotics pets.
3. Emergency Services: Disaster recovery, Earth quakes.
4. Sensor Network: Earth activities, Remote weather for sensors.

Security is a major issue in MANETs

An ID is a second protection for MANETs security. An intrusion detection system is system software used to analyze malicious behaviors network and generate reports. It can be defined as a process of monitoring the events occurs in the computer system or network and analyzing for an intrusions dealing with confidentiality, integrity and availability of a computer system.

Components of IDS [02]

1) Data Collection
2) Intrusion detection system
3) ponse Engine

For Adhoc Networks intrusion detection and response system should be both distributed and cooperative to overcome the challenges of dynamic topology.

Architecture of IDS

IDS architecture of compose of three process, monitoring, detection and response as shown in figure-

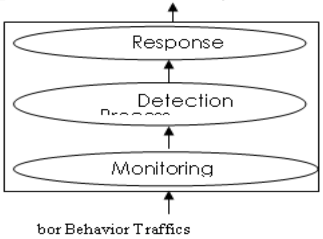

Fig: 1 Architecture of IDS

Attacks are major issues in mobile security

In mobile Adhoc-networks, there are two types of Attacks, Active and Passive attack. In active attack, the attacker distributes the performance of the network steel important information and tries to destroy the data during the exchange in the network .In passive –attack, it listens to the network in order to the know and understand how they are located in the network, How the nodes are communicating with each other. Before the attacker start an attack against the network, the attacker has enough information about the network that can easily capture an introduce attack in the network [7]. Gray hole attack is a active attack in which the attackers mislead the network by approving to forward the packets in the network. It receives the packets from the neighboring node, the attacker falls the packet. In this the attacker nodes behave usually and reply true RREP messages to the node that's started RREQ messages. When it receives the packet it starts falling the packets and lunch denial of service (DOS) attack[9]. Gray hole attack is harder to find because of data packets reached the destination and destination thinks that it is the full data. Gray hole attack in routing protocol occur at a time of routing the data packet. This attack generally occurs due to the dynamic nature of MANETs[12].

Tele:
E-mail address: er.sharma04@gmail.com

Research Gap

According to Authors [6] if the node detects a gray hole node. It makes a black list that contains information about the particular node. According to the proposed mechanism of the author, it will reduce the overheads, but if each node will detects the same node for the gray hole, it will increase the overheads rather than decreasing it. Rather it should be broadcasted to all the concerned relaying node thus reducing the number of computations for grey hole detection.

The problems of the following approach are:

- Energy Issue
- Memory Issue
- Delays

Proposed Model

Sequenced Queue based Routing Algorithm (SQRA) is proposed for Detection and Correction of Grey Hole attack by Implementing Intrusion Detection System. In this, the Detection of grey hole attack & Implements of corrective measures against it. Recovering system operation for grey hole attack. Implementing Sequenced Queue based Routing Algorithm for new routing table. Direct link established after recovering the attacks. The working of our algorithm is based on detection of broadcast IDs stored in the routing table of various intermediate nodes. The working of various nodes whoever depends upon how fast IDS responded to partially query and thus there is always a problem of overhead that may be encountered but our IDS we have limited this problem to much extend by using the application of distance vector routing algorithm. The approach and pseudo code of our algorithm has explained in next section.

Algorithm

```
Step1: For (Ring Search! = Finish)
Step 2: Send RREQs
Step 3: Receive RREPs
Step 4: Formulize Routing Table
a. Mark light link between Node & IDS
b. Formulize IDS Table
Step 5: Filter Traffic
Step 6: Analyze Traffic
Step 7: Echo Gray Hole (Nodes)
Step 8: Exit
Grey Hole (Nodes)
1. If(SSID || DID != found (Destination packet_header))
{Node_attack (sender)
Formalize ()
}Else
{Break
}Echo off
Exit
Node_attack (sender)
If sender_ACK not receive
{Node_unauthorize
Node_correct ( )
}Else
{Break
}Exit
Node_correct ( )
If Node_unauthorize (node)
Send ACK
Receive Broadcast ID-node
Update Routing table
Channel_encorporated ( Node reconfigured)
Node-UP
Node-Corrected
Exit
 Formalize ()
1. routing_table(SSID||DID)
2. Recieve Ack.
3. Node_Attack(SSID)
4. exit
```

Numerical Computations

Number of failures:

here P= number of network failures, E(D) is the excess transmission duration over distance D, F(X) is function dependent upon time and distance between two routing nodes x, V is the time range which will be infinite till transmission continues, y is the initial simulation time.

Average network life time:

Nlf= Wait time + Avg routing time

Avg routing time = (Time to transmit a packet * number of packets)*Number of Nodes transmitting

Wait time= Network halt time + Avg delays …… (ii)

Average Packet Delivery Ratio:

(Number of packets successfully transmitted / Total Number of packets transmitted) …….. (iii)

Packet drop Raito:

(Total Number of packets transmitted-Number of packets successfully transmitted)/Total Number of successful transmitted ……. (iv)

Throughput:

Normalized Routing Load/Simulation Time

*Normalized Routing Load= Total Load-(Successful Transmission/Failure)*No of transmission * no of Nodes …. (v)

Routing Overhead

Load Failed/Total Load …… (vi)

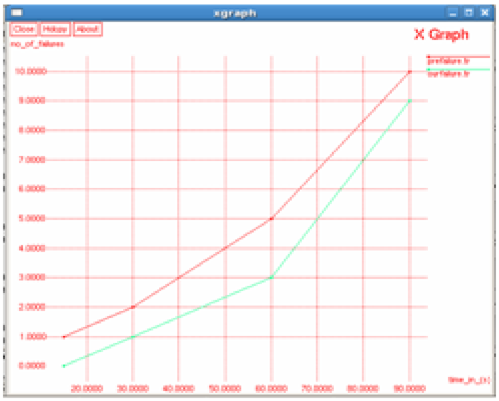

Figure 2: Comparison Graph of Number of Failures

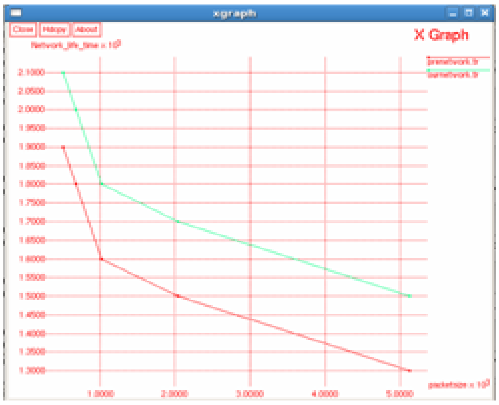

Figure 3: Comparison Graph of Average Network Lifetime

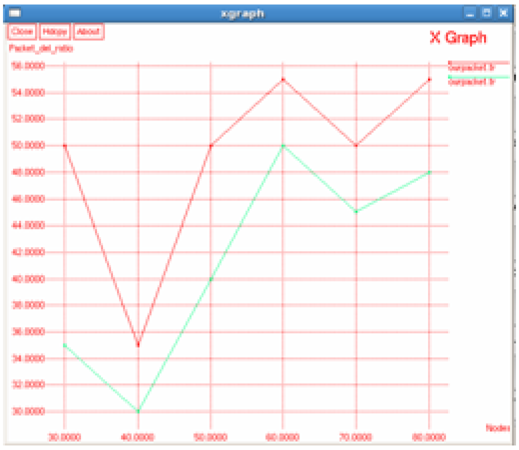

Figure 4: Comparison Graph of Packet Delivery Ratio

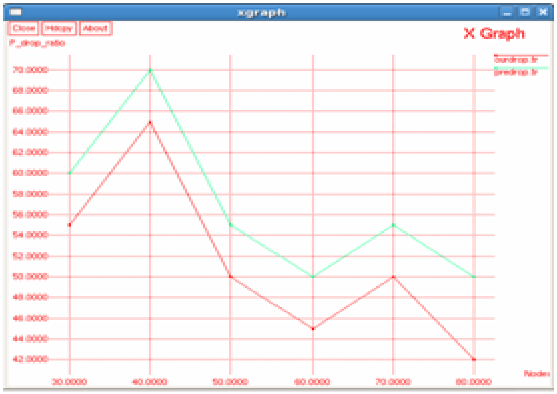

Figure 5: Comparison Graph of Packet drop Ratio

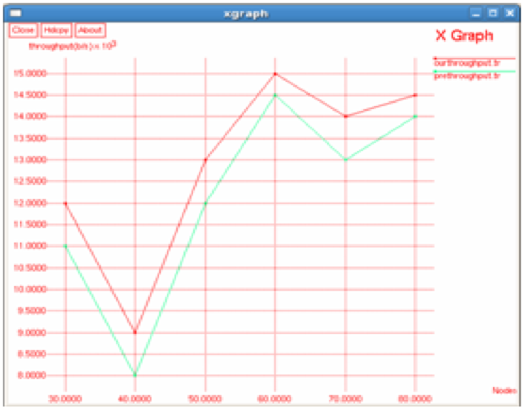

Figure 6: Comparison Graph of Throughput

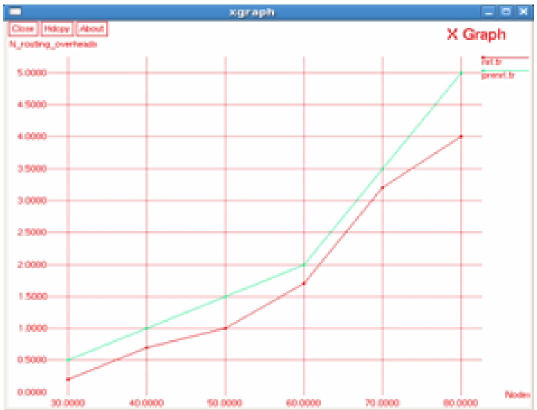

Figure 7: Comparison Graph of Routing Overhead

Table 1: comparison between previous & current results

Parameters	Previous Results	Current Results
Number of failures	4.5 packets	3.2 packets
Average network life time	1700 ms	1800 ms
Average Packet Delivery Ratio	40 packets	50 packets
Packet drop Raito	55 packets	50 packets
Throughput	11000byte/sec	13000byte/sec
Routing Overhead	1.5 sec	1.3sec

Note: All the comparison is based on 50 nodes.

Results and Graphs

The result is carried out by NS-2Simulator using following

Parameters

- ➢ umber of failure
- ➢ Average network life time
- ➢ Average packet delivery ratio
- ➢ Average packet drop ratio
- ➢ Throughput
- ➢ Routing Overhead

The results are based upon the following metrics and the graphs have been taken by using NS2 Simulator.

Conclusions:

In the paper work has been carried out on detection of gray hole and taking corrective measures against the attack. The paper include comparative analysis of the proposed technique with previous work on the basis of no. of failures, Average network life time, Average packet delivery ratio, Average packet drop Ratio and throughput. There has been improvement of 25% approx in the overall technique. In future, work can be carried for improving dynamicity of the technique and can be analyzed on the real time scenarios

Reference

[1]. Marjan Kuchaki Rafsanjani, Ali Asghar Khavasi, Ali Movaghar, 'An Efficient Method for Identifying IDS Agent Nodes by Discovering Compromised Nodes in MANET,' 2009 IEEE Second International Conference on Computer and Electrical Engineering,' PP 625-629

[2] Xia Ye, Junshan Li, Rong Luo," Hide Markov Model Based Intrusion Detection and Response for Manets", 2010 Second International Conference on Information Technology and Computer Science, 2010, IEEE, pp 142-145

[3] Onkar V.Chandure, V.T.Gaikwad,' Detection & Prevention of Gray Hole Attack in Mobile Adhoc Network using AODV Routing Protocol,' International Journal of Computer Applications (0975 - 8887) Volume 41- No.5, March 2012,' pp 27-32

[4] Shivani Sharma, Tanu preet singh,' An Efficient Intrusion Detection System for Routing Attacks in MANETs: An Analytical Report,' International Journal Of Advanced And Innovative Research (Ijair), Vol 1, issue 4 (September) , pp 213-217

[5] Shivani Sharma, Tanu preet singh,' Distance Vector Routing Algorithm for Detection and Correction of Black & Grey Hole Attack by Implementing IDS' International journal of computing Technologies, Vol 1, issue 7 (November) , pp 1-6

[6] Ashok M. Kanthe , Dina Simunic, Ramjee Prasad (2012),'A Mechanism for Grey Hole Attack Detection in Mobile Ad-hoc Networks', International Journal of Computer Applications (IJCA), Vol 53, No 16, pp 23-30.

[7] B. Revathi , D. Geetha ," A survey of cooperative black and gray hole attack in MANET", 'International Journal of

Computer Science and Management Research',Vol 1 ,Issue 2, sept 2012, pp 205-208

[8] K.S. Sujatha, Vydeki Dharmar, "Design of genetic algorithm based IDS for MANET", 'IEEE, ICRTIT- 2012,' pp 28-33

[9] Avenash Kumar, Meenu Chawla," Destination based group gray hole attack detection in MANET through AODV", 'International journal of computer science', 'Vol 9, Issue 4, No 1, July 2012, pp 292-295

[10] Pravin Ghosekar, Girish Katkar," Mobile Adhoc Networking: Imperatives and Challenges", 'IJCA Special Issue,'2010, pp 153-158

[11] Jaydip Sen, Girish Chandra," Mechanism for the detection of gray hole attack in mobile Adhoc Networks",'IEEE',2007

[12] Animesh Kr Trivedi, Rajan Arora, "A Semi distributed Reputation based Intrusion Dection System for Mobile Adhoc Networks", 'Journal of Information Assurance and Security ', 2006 , pp 265-274