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

Adoc Network

Elixir Adoc Network 60 (2013) 16090-16094

ISSN: 2229-712X

Distance Vector Routing Algorithm for Detection and Correction of Grey & Black Hole Attack by Implementing IDS

Shivani Sharma and Tanu Preet Singh

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

ARTICLE INFO

Article history:

Received: 6 November 2012;

Received in revised form:

15 June 2013;

Accepted: 27 June 2013;

Keywords

MANETs,

Grey hole attack,

Black hole attack.

ABSTRACT

Mobile Ad hoc 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 we proposed new distance vector routing algorithm (DVRA) for detecting and correcting the black hole and grey hole attack made by intruding nodes.

Introduction

Mobile Ad hoc 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 [1,11]. MANET is one of the most important technologies that have gained interest due to recent advantages in both hardware and software techniques. MANET technology allows a set of mobile uses equipped with radio interfaces (Mobile nodes) to discover each other and dynamically form a communication network. MANET incorporates routing functionality into mobile nodes so that they become capable of forwarding packets on behalf of other nodes and thus effectively become the infrastructure. Providing multiple routing paths between any source-destination pair of nodes has proved to be very useful in the context of wired networks [3,11].

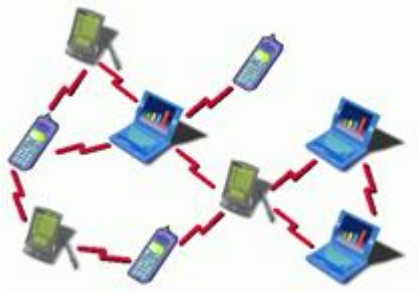


Fig 1: Typical Mobile ad-hoc network Diagram

Intrusion Detection Systems [10] help information systems prepare for, and deal with attacks. They accomplish this by collecting information from a variety of systems and network sources, and then analyzing the information for possible security problems.

Intrusion detection provides the following:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Statistical analysis of activity patterns based on the matching to known attacks
- Abnormal activity analysis
- Operating system audit

There are three main components to the Intrusion detection system

- Network Intrusion Detection system (NIDS) – performs an analysis for a passing traffic on the entire subnet. Works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of knows attacks. Once the attack is identified, or abnormal behavior is sensed, the alert can be send to the administrator.

Example of the NIDS would be installing it on the subnet where you firewalls are located in order to see if someone is trying to break into your firewall

- Network Node Intrusion detection system (NNIDS) – performs the analysis of the traffic that is passed from the network to a specific host. The difference between NIDS and NNIDS is that the traffic is monitored on the single host only and not forthe entire subnet. The example of the NNIDS would be, installing it on a VPN device, to examine the traffic once it was decrypted. This way you can see if someone is trying to break into your VPN device
- Host Intrusion Detection System (HIDS) – takes a snap shot of your existing system files and matches it to the previous snap shot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. The example of the HIDS can be seen on the mission critical machines, that are not expected to change their configuration

In Black attack [8,11] an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been

Tele:

E-mail addresses: er.sharma04@gmail.com

able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can drop the packets between them to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack. Gray Hole attack is the attack on the adhoc network. Gray Hole attack can be act as a slow poison in the network side means we can't said that probability of losing the data.

In Gray Hole Attack [9,11] a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets.

Gray Hole nodes in MANETs are very effective. Every node maintain a routing table that stores the next hop node information for a route a packet to destination node , When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in its routing table. Otherwise, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination.

Our System Model

Our distance vector routing algorithm is an advance version of tradition reactive routing algorithm with the capability of intrusion detection for grey and black hole 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

1. While (Ring Search != Finish)
2. Send REEQs
3. Receive RREPs
4. Formulize Routing Table

a. Mark light link between Node & IDS

b. Formulize IDS Table

5. Filter Traffic
6. Analyze Traffic
7. Echo Black Hole (Nodes)
8. Echo Gray Hole (Nodes)
9. Exit

Black Hole (Nodes)

1. Maintain Routing Destination
2. Check for broadcast ID, map destination address
3. Get MAC(Physical IP Address)
4. If Node_unauthorize ()

{
Send Connection_signal ()
}
Else
Exit

5. Echo off

Node_unauthorize ( )
{

(A) If (Table_Routing (Broadcast ID! =found))

{
Node-Black Hole
Node-correct ( )
}

(B) Else
Exit (Black hole (Node))

Grey Hole (Nodes)

1. If(SSID || DID != found (Destination packet_header))

{
Node_attack (sender)
Formalize ()
}
Else
{
Break
}

2. Echo off

Exit
Node_attack (sender)
If sender_ACK not receive
{
Node_unauthorize
Node_correct ( )
}
Else
{
Break
}
Exit
Node_correct ( )

1. If Node_unauthorize

Send ACK
Receive Broadcast ID
Update Routing table

2. Channel_encorporated (Node reconfigured)

{
Node-UP
Node-Corrected

3. Exit

Description of our algorithm

1. Ring search is performed for determining the location and maintain routing table for various nodes in the network
2. After maintaining the routing table and analysis the traffic. Two functions black hole and grey hole are called by arguments that detect the particular type of attacks.
3. Black Hole: This portion of the algorithm is on the basis of mobile IP and physical address along with broadcast ID is used to detect the black hole attack followed by calling the function for correcting the node.

Grey Hole: This portion of the algorithm is used to correct the grey hole by the comparing the source IDs and destination IDs with those packet headers followed by the acknowledgement and calling the node correct function.

On this particular portion of the algorithm the nodes are made UP by the channel and encorporated and node reconfiguration

Nam Animation Analysis

Nam Animations

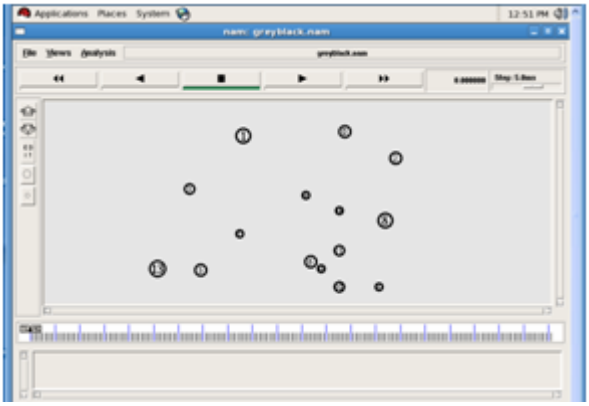


Fig 1: Initial Manets Structure

Fig 2: Normal Transmission between two nodes

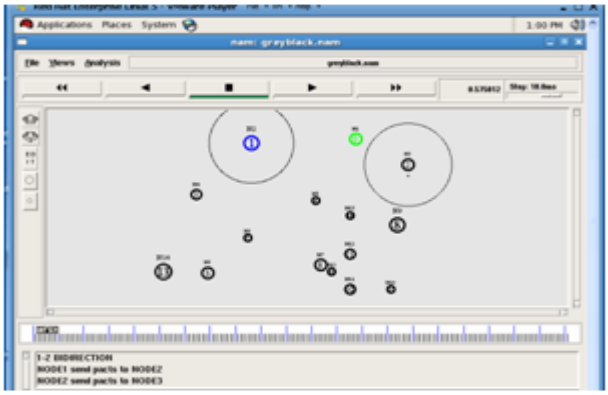


Fig 3: Packet Capturing by unauthorized node

Fig 4: Data transmission during packet capturing

Fig 5: Black hole attack detected

Fig 6: Removal of black hole and transmission enhanced

Fig 7: Detection of grey hole attack

Fig 8: Detection of grey hole & Implementing Corrective measures

Fig 9: Recovering system operation for Black and grey hole attack

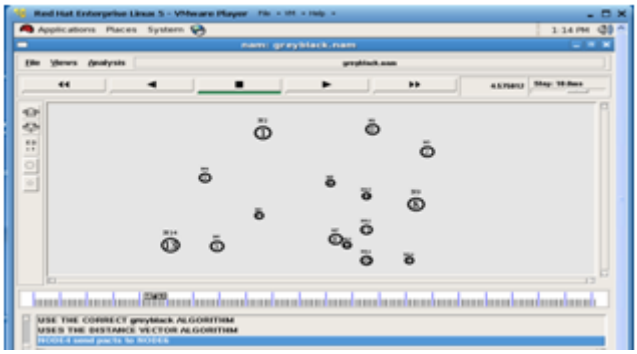


Fig 10: Implementing Distance vector algorithm for new routing table

Fig 11: Direct link established after recovering the attacks

Fig 12: IDS implementation on NODE 6

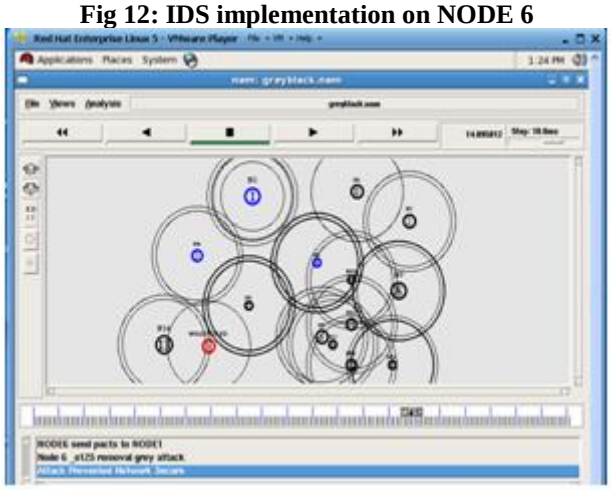


Fig 13: Transmission improved & network secured

Results And Analysis

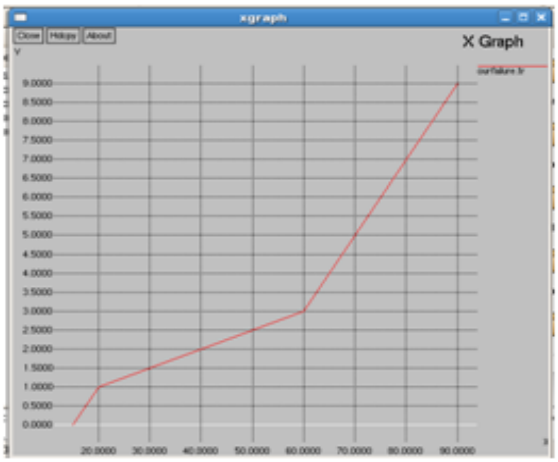
The result is carried out by NS-2Simulator using following Parameters & Metrics.

Parameter	Value
Dimensions	1500X1500 sq. m.
Number of Nodes	5,25,50,75
Simulation Time	200 s
Source Type	CBR
Number of Connections	4,10,14,25
Packet Size	512 bytes
Mac Layer	IEEE 802.11 b
Traffic Buffer Size	512,682,1024,2048 packets
Propagation Radio Model	Two Ray Ground
Physique layer	Band width as 2 Mb/s
Maximal Speed	10 m/s
Pause Time	10 s
Interval Time To send	2 packets /s

Number of Failure

Y Axis: No of failures

X Axis: Simulation Time



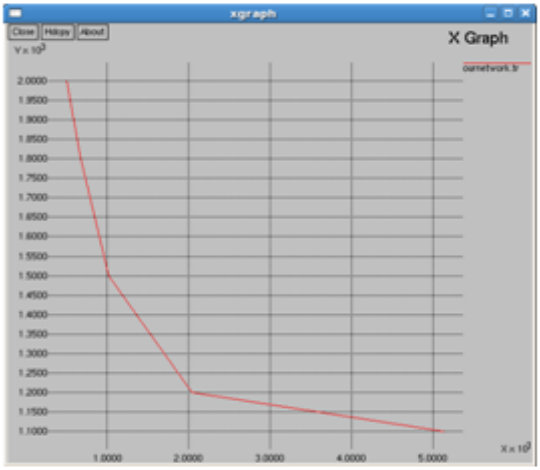
Graph 1

Graph 1 gives the analysis between the number of failures and simulation time

Average Network life time: It is the time that the first node failure happens

Y Axis: Network life time

X Axis: Traffic (in bytes)



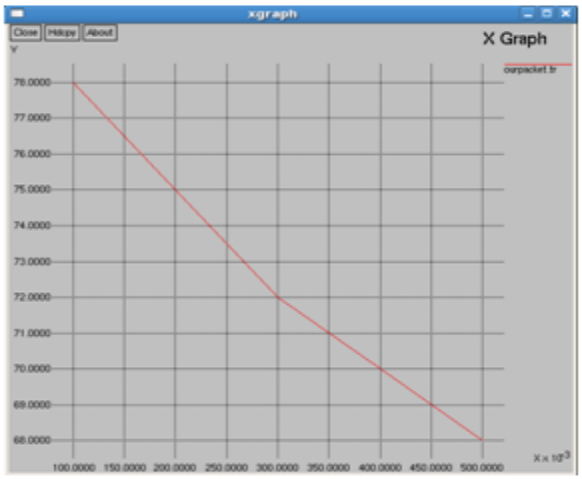
Graph 2

Graph2 gives the analysis between the network life time and Traffic (in bytes)

Average packet delivery ratio: the ratio of the number of delivered data packet to the destination.

Y Axis: Packet delivery

X Axis: Pulse rate



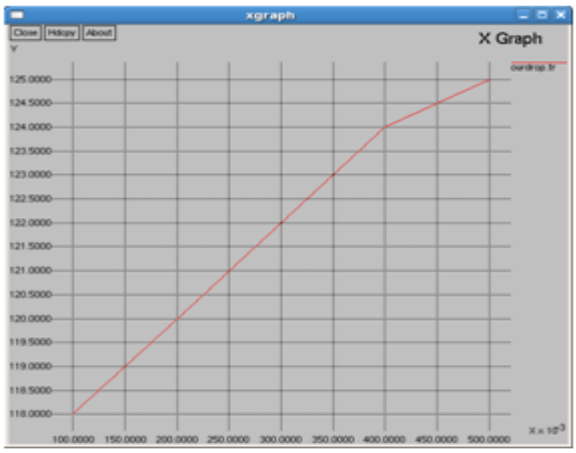
Graph 3

Graph3 gives the analysis between the Packet delivers and Pulse rate

Packet drop ratio: The number of packets originated by the source but fails to reach the destination node.

Y Axis: Dropped packets

X Axis: Pulse rate



Graph 4

Graph4 gives the analysis between the Packet drops and Pulse rate

Conclusions:

The paper presents the real time approach for prevention and detection of grey and black hole attacks. The papers shows the working of our algorithm, however comparison will be shown as future work of our work. The paper presents the ideology to allocate proper addressing for nodes that will enhance the performance by preventing against defined attacks.

References

[1] Neeraj Nehra, R.B. Patel, V.K. Bhat, 'Routing with Load Balancing in Ad Hoc Network: A Mobile Agent Approch', 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 1007), 2007 IEEE

[2]. Tameen Eissa, Shukor Abd Razak, Md Asri Ngadi. (2009),'Enhancing MANET security using Sceret public Keys', International Conference on Future Networks, IEEE, pp 130-134

[3]. 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

[4]. Nan Kang, Elhadi M. Shakshuki, Tarek R. sheltami. (2011),'Detecting forged Acknowledged in MANETs', International Conference on Advance Information Networking and Applications, IEEE, pp 488-494

[5]. S. Mangai and A. Tamilarasi. (2011), 'Analysis of an efficient Scalable and secured Geographic Routing Protocol for MANETs', International Journal of Advanced Computing (IJAC), Vol 3, issue 2, pp 47-53

[6]. Okoli Adaobi, Ejiro Igbesoko, Mona Ghassemian. (2012),' Evaluation of Security Problems and Intrusion Detection Systems for Routing Attacks in Wireless Self-organised Networks', IEEE

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay,' Different Types of Attacks on Integrated MANET-Internet Communication,' International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), pp 265-274

[8] Pradip M. Jawandhiya et. al.' International Journal of Engineering Science and Technology,' Vol. 2(9), 2010,' pp 4063-4071

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

[10]http://www.sans.org/reading_room/whitepapers/detection/understanding-intrusion-detection-systems_337

[11] 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