UACEE International Journal of Advances in Computer Networks and its Security – IJCNS
Volume 3 : Issue 2 [ISSN 2250 – 3757]
Publication Date : 05 June 2013

Sequenced Queue based Routing Algorithm (SQRA) for Detection and Correction of Grey Hole Attack by Implementing IDS

Er. Shivani Sharma, Er. Tanu Preet Singh

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 Sequenced Queue based Routing Algorithm (SQRA) for Detection and Correction of Grey Hole attack by Implementing Intrusion Detection System

***Keywords*: MANETs, Grey hole attack, IDS**

I. 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].

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

Gray Hole Attack [9, 11, 12] 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.

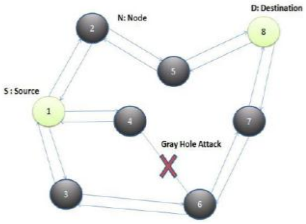


Figure 1: Gray Hole Attack in Mobile Adhoc Network

Shivani Sharma
Assistant Professor,
Department of Computer Science & Engineering
Amritsar College of Engineering & Technology,
Amritsar, INDIA
er.sharma04@gmail.com

Tanu Preet Singh
Associate Professor,
Department of Computer Science & Engineering
Amritsar College of Engineering & Technology,
Amritsar, INDIA
tanupreet.singh@gmail.com

II. Our System Model

Our 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 & Implementation of corrective measures. Recovering system operation for grey hole attack. Implementing Sequenced Queue based Routing Algorithm for new routing table. Direct link established after recovering the attacks. Implementation of Intrusion detection system. 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.

A. 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 Grey Hole (Nodes)
8.  Exit
```

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
```

III. Nam Animation Analysis

A. Nam Animations

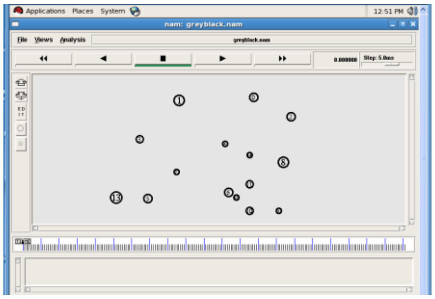
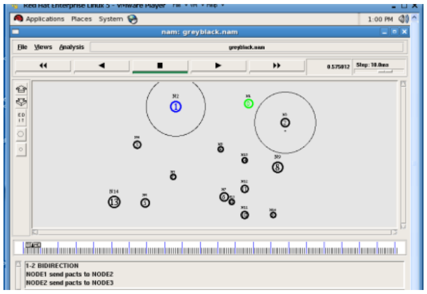
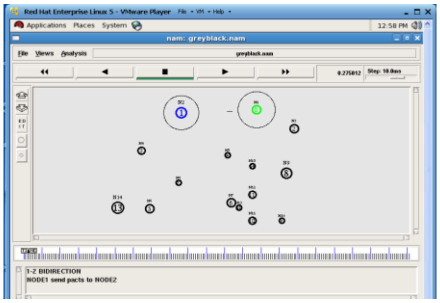


FIG 2: Initial Manets Structure



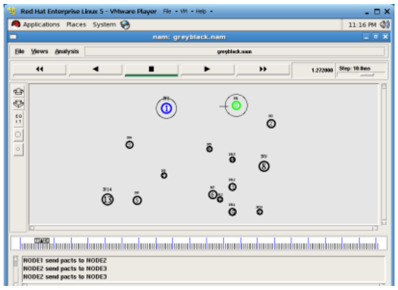
1-2 BIDIRECTION
NODE1 send pacts to NODE2
NODE2 send pacts to NODE3

FIG 3: Normal Transmission between two nodes


Red Hat Enterprise Linux 5 - VMware Player
Applications Places System
nam: greyblack.nam
File Views Analysis
greyblack.nam

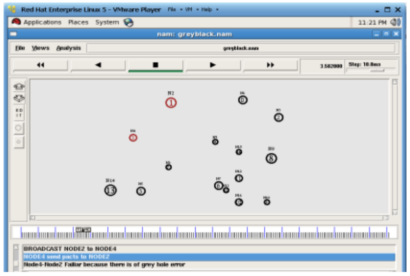
1-Z BIDIRECTION
NODE1 send pacts to NODE2

FIG 4: Packet Capturing by unauthorized node



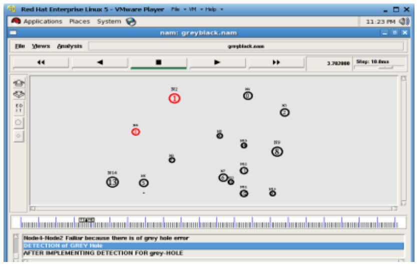
```
NODE1 send pacts to NODE2
NODE2 send pacts to NODE3
NODE2 send pacts to NODE3
```

FIG 5: Data transmission during packet capturing



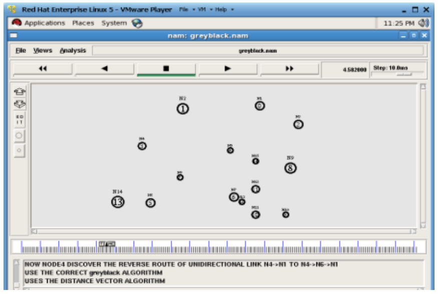
```
BROADCAST NODE2 to NODE4
NODE4 send pacts to NODE2
Node4-Node2 Failar because there is of grey hole error
```

FIG 6: Detection of grey hole attack



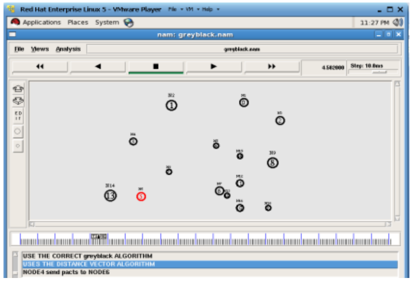
```
Node4-Node2 Failar because there is of grey hole error
DETECTION of GREY Hole
AFTER IMPLEMENTING DETECTION FOR grey-HOLE
```

FIG 7: Detection of grey hole & Implementing Corrective Measures



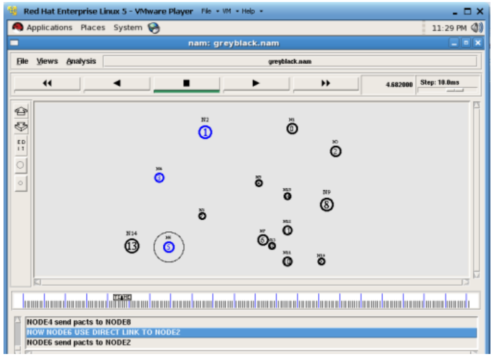
```
NOW NODE4 DISCOVER THE REVERSE ROUTE OF UNIDIRECTIONAL LINK N4->N1 TO N4->N6->N1
USE THE CORRECT greyblack ALGORITHM
USES THE DISTANCE VECTOR ALGORITHM
```

FIG8: Correction of grey hole attack by implementing of algorithm



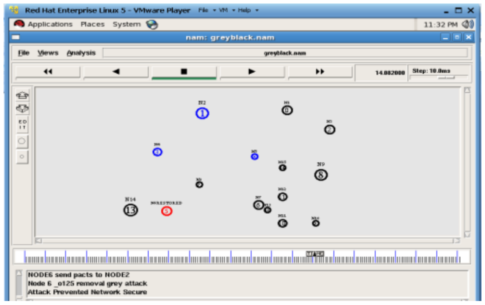
```
USE THE CORRECT greyblack ALGORITHM
USES THE DISTANCE VECTOR ALGORITHM
NODE4 send pacts to NODE6
```

FIG9: Implementation of Sequenced Queue based Routing Algorithm for new routing table



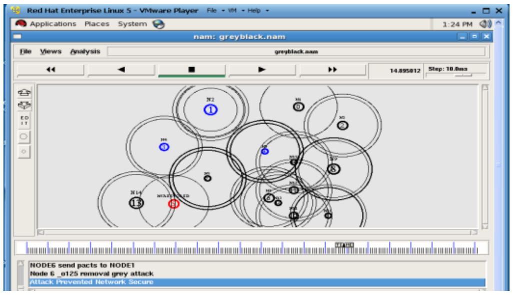
```
NODE4 send pacts to NODE8
NOW NODE6 USE DIRECT LINK TO NODE2
NODE6 send pacts to NODE2
```

FIG 10: Direct link establish after recovering the attack



```
NODE6 send pacts to NODE2
Node 6 _o125 removal grey attack
Attack Prevented Network Secure
```

FIG11: IDS Implementation on Node 6



```
NODE6 send pacts to NODE1
Node 6 _o125 removal grey attack
Attack Prevented Network Secure
```

Fig 12: Transmission improved & network secured

IV. Results and Analysis

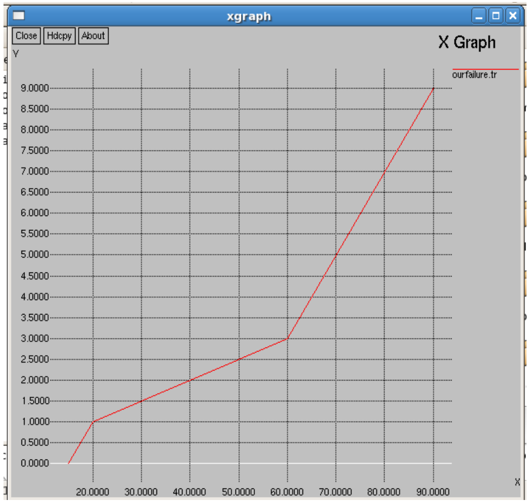
A. The result is carried out by NS-2Simulator using following Parameters

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

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

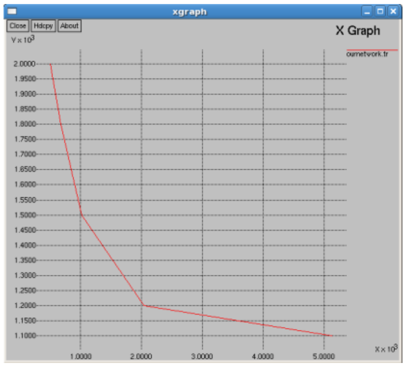
- ➢ Number of failure
- ➢ Average network life time
- ➢ Average packet delivery ratio
- ➢ Average packet drop ratio
- ➢ End to End Delay
- ➢ Throughput
- ➢ Normalized Routing Load
- ➢ Routing Overhead

1. Number of Failure



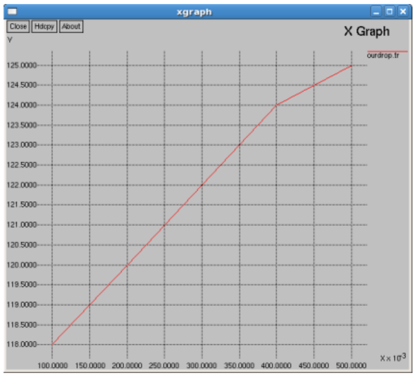
Graph 1 gives the analysis between the number of failures and simulation time

2. Average Network life time



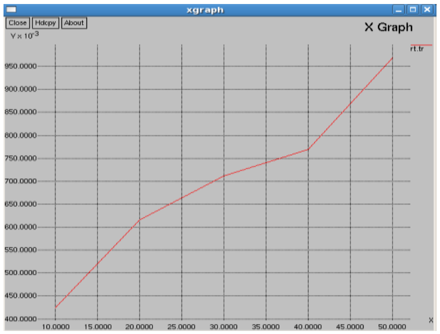
Graph2 gives the analysis between the network life time and Traffic (in bytes)

3. Average packet delivery ratio



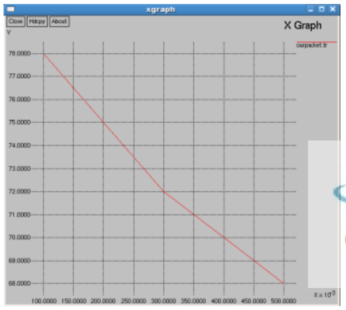
Graph3 gives the analysis between the Packet delivers and Pulse rate

4. Packet drop ratio



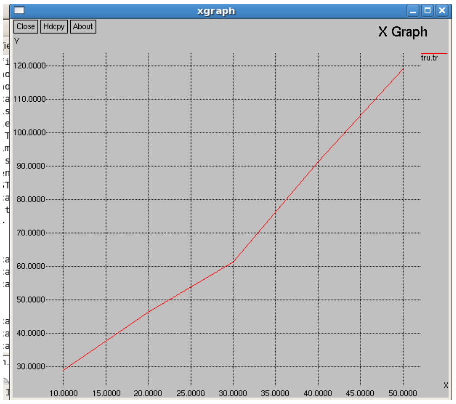
Graph4 gives the analysis between the Packet drops and Pulse rate

5. End to End Delay



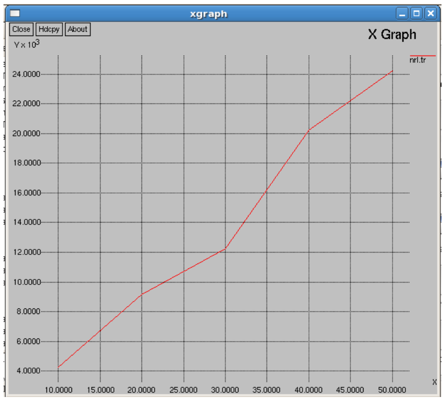
Graph 5 gives the analysis the of end to end delays

6. Throughput



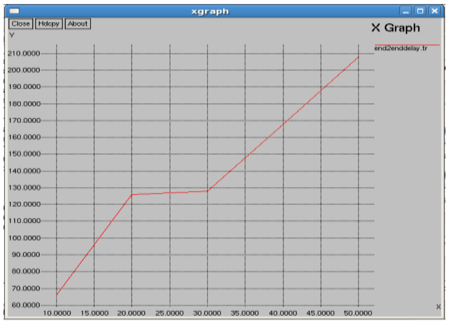
Graph 6 gives the analysis of the throughput

7. Normalized Routing Load



Graph 7 gives the analysis of the normalized Load

8. Routing Overhead



Graph 8 gives the analysis of routing overhead

V. Conclusions

The paper presents the real time approach for detection and correction of grey attack by Implementing Intrusion Detection System. The Detection of grey hole attack & Implementation of corrective measures. Recovering system operation for grey hole attack. Implementing Sequenced Queue based Routing Algorithm for new routing table. Direct link established after recovering the attacks. Implementation of Intrusion detection system. 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 forRouting 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

[12] 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