IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 5, May 2016.
www.ijiset.com
ISSN 2348 – 7968

Detection of Malicious Nodes in Routing Of Mobile AdHoc Network

Bhavik Panchal[1]

[1] ME Wireless & Mobile Computing, GTU PG SCHOOL Ahmedabad, Gandhinagar, Gujarat, India

Abstract

To find method of detecting selfish and misbehaving node for providing better security in routing of adhoc network. First of all generate the adhoc network. In Adhoc network nodes are mobile so the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering routing messages is executed by the nodes themselves, so one or more of them may misbehave and disturb the network. The misbehavior or attack can be of many types.

In the network the node can work in two ways by exhibiting selfishness or misbehaviour and cause disturb once in the network by using different type of attack. To identify or detecting malicious or selfish node Intrusion Detection System (IDS) system is developed. It has different architecture for to detect malicious or selfish node. One is Stand Alone architecture and other is Distributed and co-operative architecture.

I will use Watch-Dog mechanism to detect selfish and misbehaving node that agree to forward packet but fails to do so. Path-rater is mechanism used for removing path from cache that contain malicious or selfish node.

Keywords: Ad-Hoc Network ,Watch-Dog , Intrusion Detection System (IDS),Security , Distributed , Stand Alone Architecture , Pathrater.

1. Introduction

During the last few years we have all witnessed a continuously increasing growth in the deployment of wireless and mobile communication networks. Mobile ad hoc networks consist of nodes that are able to communicate through the use of wireless mediums and form dynamic topologies. The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations like the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority since one does not exist. Therefore, a network layer protocol designed for such self-organized networks must enforce connectivity and security requirements in order to guarantee the undisrupted operation of the higher layer protocols.

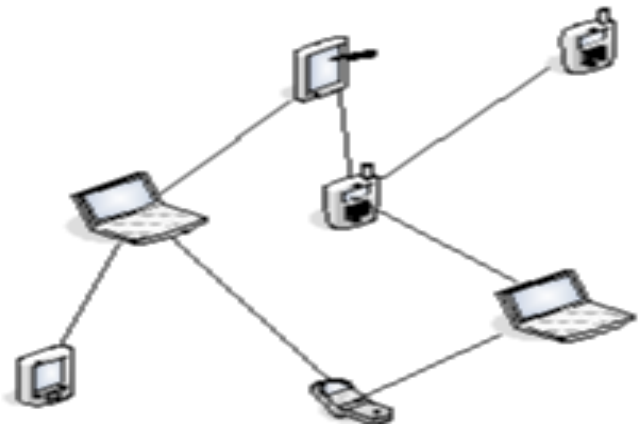

Figure 1.1 Ad-Hoc Network Sample

Security is an essential service for wired and wireless network communications. The success of mobile ad hoc networks (MANET) strongly depends on peoples confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, and non-repudiation. We provide a survey on attacks and countermeasures in MANET in this paper. The countermeasures are features or functions that reduce or eliminate security vulnerabilities and attacks. First, we give an overview of attacks

ISSN 2348 – 7968

according to the protocols stacks, and to security attributes and mechanisms.

2. Proposed Work Flow

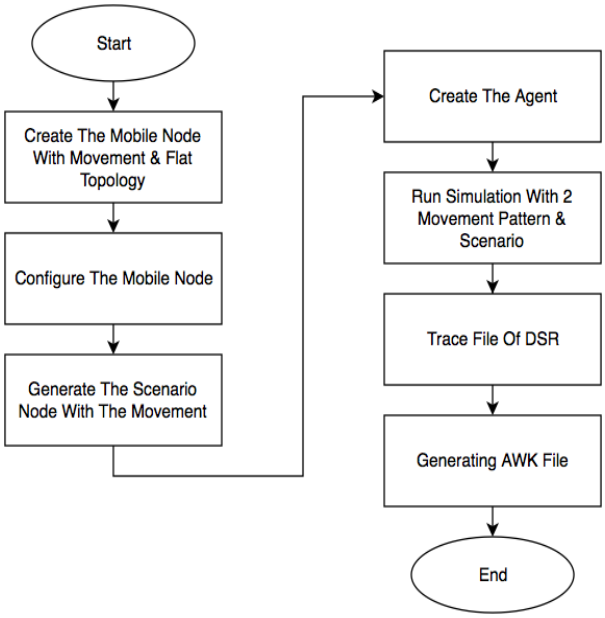

Figure 2.1 Flow Diagram

3. Mechanism

Xia Wang [11] describes the various IDS system with different mechanism that used for detection of node.

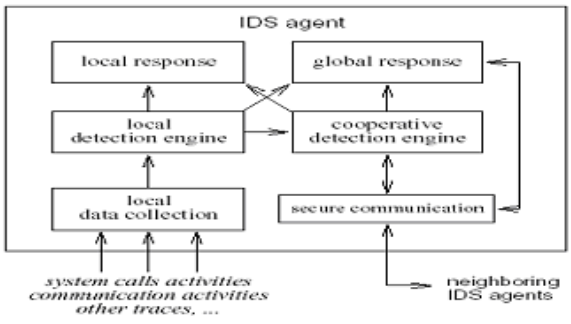

Figure 3.1: Distributed and cooperative architecture component

In the IDS system the mechanism is used to identify or detect the node in network. The different mechanisms are used with different architecture and according to different routing protocol mechanism is change. We have to first check that which architecture used in network for IDS and also which routing protocol is used in network In that stand alone architecture we are using Watchdog and Pathrater.[12]

Watchdog

Every node that participates in the ad hoc network employs the watchdog functionality in order to verify that its neighbors correctly forward packets. When a node transmits a packet to the next node in the path, it tries to promiscuously listen if the next node will also transmit it. Furthermore, if there is no link encryption utilized in the network, the listening node can also verify that the next node did not modify the packet before transmitting it.

The watchdog of a node maintains copies of recently forwarded packets and compares them with the packet transmissions overheard by the neighboring nodes. Positive comparisons result in the deletion of the buffered packet and the freeing of the related memory. If a node that was supposed to forward a packet fails to do so within a certain timeout period, the watchdog of an overhearing node increments a failure rating for the specific node.

Pathrater

The pathrater assesses the results of the watchdog and selects the most reliable path for packet delivery. One of the base assumptions of this scheme is that malicious nodes do not collude in order to circumvent it and perform sophisticated attacks against the routing protocol.

The pathrater extension to DSR selects routes for packet forwarding based on the reliability rating assigned by the watchdog mechanism. Specifically, a metric for each path is calculated by the pathrater by averaging the reliability ratings of the nodes that participate in the path. This path metric allows the pathrater to compare the reliability of the available paths, or to emulate the shortest path algorithm when no reliability ratings have been collected. The pathrater selects the path with the highest metric when there are multiple paths for the same destination node.

4. Security Scheme

There are two main approaches in securing ad hoc environments currently utilized.

The first approach is the intrusion detection approach that aims in enabling the participating nodes to detect and

ISSN 2348 – 7968

avoid malicious behaviour in the network without changing the underlined routing protocol or the underling infrastructure. Although the intrusion detection field and its applications are widely researched in infrastructure networks it is rather new and faces greater difficulties in the context of ad hoc networks.

The second approach is secure routing that aims in designing and implementing routing protocols that have been designed from scratch to include security features. Mainly the secure protocols that have been proposed are based on existing ad hoc routing protocols like AODV and DSR but redesigned to include security features. In the following sub sections we briefly present the two approaches in realizing security schemes that can be employed in ad hoc networking environments.

5. Proposed Solution

1. Used Random Waypoint Model

Each node chooses a random destination and moves towards it with a random velocity chosen from [0, Vmax] After reaching the destination, the node stops for a duration defined by the ”pause time” parameter After this duration, it again chooses a random destination and repeats the whole process again until the simulation ends
Parameters: Max Velocity Vmax, Pause time T

2. Create Mobile Node

A mobile node is created using the following procedure:

```
for { set j 0 } { $j < $opt(nn) } { incr j }
{
set node ( $j ) [ $nsnode ]
$node ( $i) random-motion 0 ; - disable random motion
}
```

3. Generate Scenario

generating a scenario with 4 nodes, moving with a maximum speed of 20m/s, with a pause time of 10s, within a topology boundary of 670 x 670, for a simulation time of 400s. We specified this scenario in a separate scenario file, scene-4-test. We generated this scenario file by typing the following command in ns-2.33/indep-utils/cmugen/setdest directory:

./setdest -n 4 -p 10.0 -M 20.0 -t 400 -x 670 -y 670 > scene-4-test

4. Create Agent

Agents are used in the implementation of protocols at various layers. They represent endpoints where network-layer packets are constructed or consumed. The different agents currently supported by NS at the transport layer like TCP, TCP Reno. NS also has routing agents implementing the different routing protocols like DSDV, TORA, AODV and DSR and for application layer we have CBR traffic agent. Once the agent is created then we have to connect different agent so communication between every layer and packet transfer is done.

$set udp [new Agent/UDP]

creates a udp agent. Users can create any agent or traffic sources in this way.

$ns attach-agent node agent

5. Run Simulation

$ns run starts the simulation.

$ns at 5.0 “finish”

6. Simulation Result

Node number	0%	20%	40%
4	0	20	26
5	0	0	30
7	0	24	30
14	0	19	21
16	0	1	23
18	0	30	40
20	0	1	25
22	0	20	30
25	0	5	32
28	0	25	28
30	0	2	30
32	0	1	27
34	0	6	43
36	0	15	23
38	0	2	30
40	0	24	27

ISSN 2348 – 7968

42	**0**	**2**	**30**
44	**0**	**38**	**41**
48	**0**	**5**	**28**
50	**1**	**1**	**20**

Table 6.1 Simulation Scenario Drop Packet Result

As Above Table 6.1 0%, 20%, & 40% misbehaviour nodes represent that, As threshold changes, detection rate also changes. Detection Rate is calculated for the scenarios.

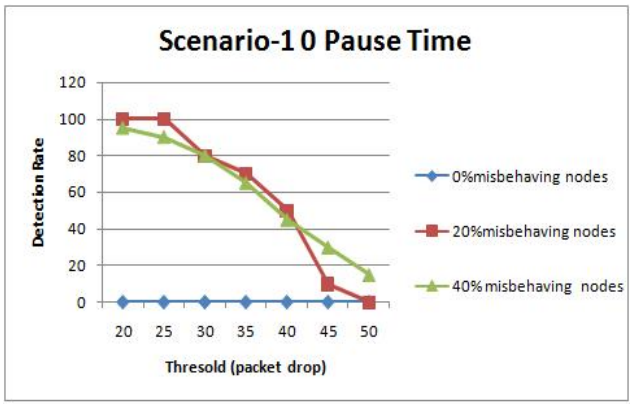

Figure 6.1 Node Detection Rate Graph

Throughput are changes according to 0%, 20%, & 40% misbehavior node. Throughput is calculated for scenario. Throughput is increase in scenarios with modification in DSR routing protocol.

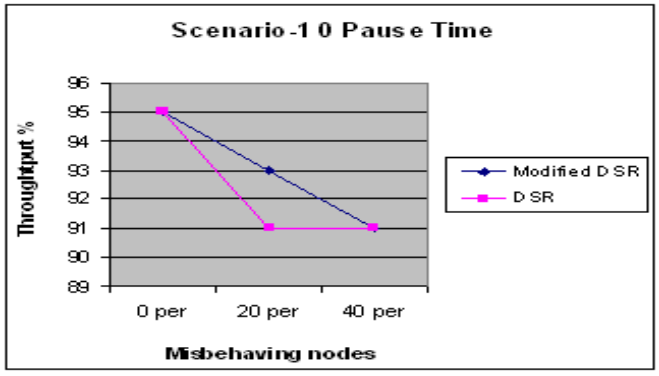

Figure 6.2 Throughput Graph

Overhead are changes according to 0%, 20%, & 40% misbehaviour node. Overhead is calculated for scenario. Overhead is decrease in scenario with modification in DSR routing protocol.

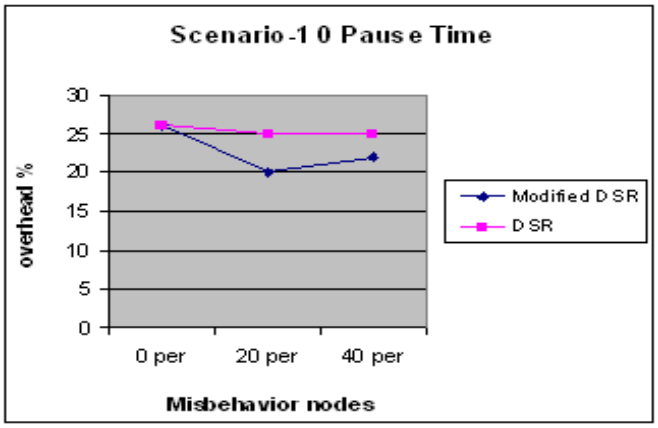

Figure 6.3 Overhead Graph

4. Conclusions

After doing parametric study for different architecture of IDS system for ad-hoc wireless network we get the different mechanism to detect the malicious or selfish node. On that Watchdog is used in Stand Alone architecture for detect in malicious or selfish node. In Distributed and Cooperative architecture we have CONFIDANT Protocol, Probing algorithm mechanism used for detection. Stand Alone architecture Watchdog mechanism made for forwarded packet drop misbehaviour done by node.

In the forwarded packet Drop misbehaviour we have to maintain rating for every node and according to rating we can identify malicious or selfish node. After detection we have to select the path for send packet that not contain in malicious or selfish node that is done by the pathrater mechanism. Path is chosen by packet properly means not contain malicious or selfish node then network performance increase and also provided the reliability.

References

[1] S. Martiet, “Mitigating routing misbehavior in mobile ad hoc networks,” ACM Mobicom, pp. 255–65, Auguest 2000.

ISSN 2348 – 7968

[2] C. Murthy and B. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols. New Delhi: Prentice Hall India, second ed., 2005.
[3] H. yang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Communications magazine, October 2000.
[4] K. Inkinen, "New secure routing in ad hoc networks," tech. rep., Helsinki University of Technology. kai.inkinen@hut.fi.
[5] D. O. Patroklos G. Argyroudis, "Secure routing for mobile ad hoc networks,"
[6] E. J. Caballero, "Vulnerabilities of intrusion detection systems in mobile ad-hoc networks - the routing problem," erjica@gmail.com.
[7] B. A. Jean-Marie Orset and A. Cavalli, "An efsm-based intrusion detection system for ad hoc networks," Institut National des Telecommunications GET-INT. Evry, France fjean-marie.orset, baptiste.alcalde, ana.cavallig@int-evry.fr.
[8] S. S. Frank Kargl, Andreas Klenk and M. Weber, "Advanced detection of selfish or malicious nodes in ad hoc networks," Auguest 2004.
[9] R. D. Ningrinla Marchang, "Intrusion detection system for wireless networks," Collaborative techniques for intrusion detection in mobile ad-hoc networks, pp. 508–523, June 2008.
[10] Y. X. G. S. Bo Sun, Osborne L, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," Wireless Communications, IEEE, vol. 14, pp. 56–63, October 2007.
[11] X. Wang, "Intrusion detection techniques in wireless ad hoc networks," Computer Software and Applications Conference, vol. 2, pp. 347–349, Sepetemer 2006. COMPSAC apos;06. 30th Annual International.
[12] T. W. Mike Just, Evangelos Kranakis, "Resisting malicious packet dropping in wireless ad hoc networks,"
[13] K. Fall and K. Varadhan, The ns Manual (formerly ns Notes and documentation). UC Berkeley, LBL, USC/ISI, and Xerox PARC. http://www.isi.edu/nsnam/ns/ns-documentation.html.
[14] NS by Example. http://nile.wpi.edu/NS.
[15] C. MonarchProject, "The cmu monarch projects wireless and mobilty extensions to ns.," Collaborative techniques for intrusion detection in mobile ad-hoc networks, October 1999. http://www.monarch.cs.cmu.edu/cmu-ns.html.
[16] Ns mailing list. ns-users@isi.edu.

ACKNOWLEDGEMENT

Though only my name appears on the cover of this Report, a great many people have contributed to its production. I owe my gratitude to all those people who have made this dissertation possible and because of whom my Dissertation experience has been one that I will cherish forever.

I am extremely grateful to my coordinator **Mr. Gardas Naresh Kumar (C-DAC)** for being a source of inspiration and for their constant support in the Design and Evaluation of the Dissertation. They have been the constant constructive force throughout my pursuit of Masters Degree at GTU-CDAC and I am sure that their active and passive teachings will always inspire me throughout my life.

I will always remain indebted to my guide at Shankersinh Vaghela Bapu Institute of Technology, Gandhinagar, Honorable **to Mr. Nitin Pandya.** I am thankful to him for his constant constructive criticism and invaluable suggestions, which benefited me a lot while doing research on Detection Of Malicious Nodes In Routing Of Mobile AdHoc Network. He has been always there to support me whenever I felt down or lost my way and always led me on right path.

I also express my gratitude to **Mr. Bhadreshsinh Gohil (GTU PG School)**, for providing me the infrastructure to carry out the Dissertation and to all staff members who were directly and indirectly instrumental in enabling us to stay committed.

I would like to thank my parents & my friends for always giving me full support, inspiring advices and courage to always follow righteous path whenever my steps have faltered.