ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Implementation of Multipath Routing Scheme for Detecting Malicious Node in MANET

Neha B. Bhoyar, Prof. Poonam P. Borkar

M.E. 2nd Year, Department of CSE, G.H. Raisoni College of Engineering & Management, Amravati, Maharashtra, India

Assistant Professor, Department of CSE, G.H. Raisoni College of Engineering & Management, Amravati, Maharashtra, India

ABSTRACT: Mobile Ad-hoc Network (MANET) consists of mobile nodes that are connected via very dynamic multi-hop channels. Routing in MANET is a challenging task. This is primarily due to their infrastructure less property of MANET. In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. This work aims to identify the malicious nodes by using the novel approach called Acknowledge Based Route Discovery (ABRD), and also to provide alternative path using multipath routing algorithm, if such malicious node/nodes detected in routing path, during the route discovery. And also maintain blacklist of such malicious nodes so that all the nodes can be alerted not to use any route in which detected malicious node is participating.

I. INTRODUCTION

Mobile Ad-Hoc Network (MANET) is an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. Two nodes out of direct communication range need intermediate nodes to forward their messages. Due to multi-hop routing and open working environment, MANETs are vulnerable to attacks by selfish or malicious nodes, such as packet dropping (black-hole) attacks and selective forwarding (gray-hole) attacks. The most target area of research in mobile ad hoc networks is to provide a trusted environment and secure communication.

Mobile means 'moving' and ad-hoc means 'temporary without any infrastructure. So, a mobile ad-hoc network consists of group of mobile nodes (each equipped with wireless transmitter, receiver and antenna), which collaborate to communicate with each other without any fixed central base station. Due to infrastructure-less nature of the network, routing and network management is done cooperatively by the nodes i.e. the nodes themselves are responsible for the creation, operation and maintenance of the network.

The topology of the network varies rapidly and unpredictably over time due to mobility of the nodes. Topology varies in the way that a group of nodes may connect together to form a large network and later they may split to form smaller groups. Performance of MANET depends upon routing protocols, battery consumption, bandwidth etc. Routing is done using various routing protocols. The open medium, dynamic characteristics and lack of central infrastructure characteristics make MANETs susceptible to various security threats that degrade the performance of the network in terms of reliability and throughput.

A MANET is a collection of mobile nodes that organize themselves into a network without any predefined infrastructure or centralized operation management. MANET is an IP based network consisting of a number of wireless and mobile machine nodes linked with radio. In MANET, nodes within the radio range communicate with each other directly via wireless links, while nodes out of the radio range need an intermediate node to forward their

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

messages.[11] All the nodes in network participate in network management task. Hence network management is done in distributed manner. Each node in the network works both as router and host. As all nodes are movable so this changes topology of the network dynamically, that brings more challenges in security of Ad hoc network. MANET does not require any fixed infrastructure such as base stations; therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously.

Dynamic network topology, fluctuating link bandwidth, multi-hop routing, self-organization, self-adaptive and self configurable make it an attractive option for broad area of networking, particularly in military tactical, personal area, instant conferences and disaster area networks. Different characteristics of MANETs include autonomous terminal, fast deployment, dynamic topology, fluctuating, bandwidth, resource constraints, lack of fixed infrastructure, self-organization, distributed operation and lack of physical security

II. RELATED WORK

Chin-Feng Lai et al, IEEE [2014]. In this paper the author tries to solve the issues of blackhole and grayhole attacks caused by malicious nodes by designing a Dynamic Source Routing (DSR) mechanism known as Cooperative Bait Detection Scheme (CBDS). It combines the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio. It achieves its goal with Reverse tracing technique. Cooperative Bait Detection scheme is proposed to detect malicious nodes in Manet for the grayhole and blackhole attacks [1]

Cooperative Bait Detection Scheme (CBDS) has been used to tackle blackhole and grayhole attacks caused by malicious nodes [1]. CBDS combines the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio. It achieves its goal with Reverse tracing technique.

Shreenath [2], proposed Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs. This work focus on improving the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to safeguard it against flooding and black hole attacks. The proposed mechanism is for flooding attack works even when the identity of the malicious nodes is unknown and does not use any additional network bandwidth. The performance of a small multicast group will degrade seriously under these types of attacks even the solution is available.

Sujatha [3], proposed Design of Genetic Algorithm based IDS for MANET. In this work a technique to analyze the exposure to attacks in AODV, specifically the most common network layer hazard, Black Hole attack and to develop a specification based Intrusion Detection System (IDS) using Genetic Algorithm approach. The proposed system is based on Genetic Algorithm, which analyzes the behaviours of every node and provides details about the attack. Genetic Algorithm Control (GAC) is a set of various rules based on the vital features of AODV such as Request Forwarding Rate, Reply Receive Rate and so on.

Konate [4], proposed an Attacks Analysis in mobile ad hoc networks: Modelling and Simulation. In this title we present work is dedicated to study attacks and countermeasures in MANET. They presented several alternatives of DOS attacks met in MANETs, their operating process thus the mechanisms used and the protocols which implement them to counter these attacks.

Gandhewar [5], proposed Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Ad-hoc Network. This work mainly focuses on sinkhole problem, its consequences & presents mechanism for detection & prevention of it on the

An Approach to Defend against Wormhole Attack in Ad Hoc Network Using Digital Signature [6]. They present a mechanism which is helpful in prevention of wormhole attack in ad hoc network is verification of digital

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

signatures of sending nodes by receiving node because each legitimate node in the network contains the digital signature of every other legitimate nodes of same network. A wormhole is one of prominent attack which is formed by two malicious nodes and a tunnel. In order to protect from wormhole attack we used the scheme called multi hop count analysis (MHA) with verification of legitimate nodes in network through its digital signature.

III. PROPOSED SYSTEM

In the project of "Implementation of Multipath Routing Scheme for Detecting Malicious Node in Manet" Module shows Topology formation, Broadcasting, Malicious Node Detection, and Detection of Attacks and finally find the shortest path which does not contain malicious nodes. Comparison has been done on the basis of the parameter like throughput, packet delivery ratio etc.

A. Topology Formation:

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network and may be depicted physically or logically. Physical topology is the placement of the various components of a network, including device location and cable installation, while logical topology illustrates how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical.

```
# Creating Topology
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
```

The above code is placed in the tcl file for the formation of the topology and placing the node on the X-Y axis.

B. Broadcasting:

Broadcasting refers to a method of transferring a message to all recipients simultaneously. Broadcasting can be performed as a high level operation in a program, for example broadcasting Message Passing Interface, or it may be a low level networking operation, for example broadcasting on Ethernet.

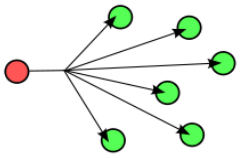

Figure: Broadcasting of message

```
set btp [open btemp w]
puts $btp "$stnd $ednd $tm $itval $src $dst $a($n)"
close $btp
exec awk -f rreq.awk btemp Neighbor KeyDetails
source bcast.tcl
set tmp [open Time r]
set tm [gets $tmp]
close $tmp
} $ns_ at 2.0 "broadcast 0 [expr $val(nn)-1] 2.0 0.1 0"
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

The above code shows the procedure of broadcasting. In broadcasting the RREQ message is send to the neighbouring node and ACK is received. It will start the broadcasting from the node 0 and up to the node 49 i.e. (nn-1). For all the broadcasting it will take 2 sec.

C. Malicious Node Detection and Attacks:

Malicious nodes seriously affect the performance of the Ad-Hoc network. The propose system will help to detect the malicious node on the basis of the packet size or the drop of the ACK. The size of the packet and the time required for the acknowledgement is set in the tcl file. In proposed system the light is thrown mainly on the three attacks i.e. blackhole, grayhole and warmhole. All the attacks are detected by using RSS algorithm in system.

D. Finding the Shortest Path:

After the detection of malicious nodes and the type of attack performed on the nodes the main objective is to find the shortest path. But the shortest path should not contain any malicious node. The shortest path find in the system by using Floyd-Warshall algorithm. The energy of the network and also the cost must be preserved by finding the shortest path in proposed system.

IV. STEPS OF PROPOSED WORK

Step 1: Initialize the node locations. Every time the node location is changed randomly.

Step2: Topology formation will be done by broadcasting topology discovery Packets.

Step 3: After topology formation broadcasting will be done. The source node broadcast the RREQ to its neighbouring nodes. The network deals with 50 mobile nodes i.e 0-49.

Step 3: Neighbouring nodes receives the RREQ and send acknowledgement to source node and forward RREQ to its intermediate nodes.

Step 4: If any node will not send the acknowledgement then that node will be detected as a malicious node.

Step 5: Attack held on nodes is detected by using RSS algorithm.

Step 6: All paths which contain malicious nodes will be rejected.

Step 7: From the remaining path shortest path will be selected by using Warshall algorithm.

V. SIMULATION RESULTS

The results for the detecting malicious node, finding the different types of attacks and finding the shortest path is simulated on NS2 i:e Network simulator -2 . It is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multicast protocols consider a network consisting of N=n sensor nodes distributed on d * d meter sq. area, all sensor nodes are configured in no beacon-enabled mode. Parameters of node are set. When the simulation is started, the first task of the scheduler is to schedule the events that are already predefined by the user in the scenario file. Thus ns TCL commands from the scenario file are scheduled first. Events like creating a new simulator object, starting nodes/traffic, node configuring, etc can be predefined, hence are scheduled first.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

hannel Type	Channel/Wireless Channel
Radio-Propagation Model	Propagation/Two Ray Ground
Network Interface Type	Phy/Wireless phy
MAC Type	Mac/802_11
Link Layer	LL
Antenna Model	Antenna/Omni antenna
Max Packet In Ifq	300
Number Of Mobile Nodes	50
Routing Protocol	AODV
X Dimension Of Topography	1670
Y Dimension Of Topography	970
Time Of Simulation End	20 sec.

Table: Parameters of ns-2

The simulation result shows that the proposed system can performed better with parameter like Packet Delivery ratio, Average Delay and Throughput than the previous system. Following figure shows comparisons between the simulation results of proposed system and existing system.

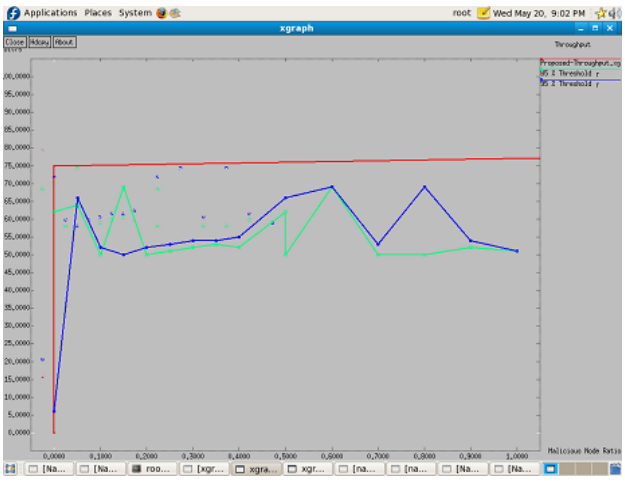

Fig.1. Throughput

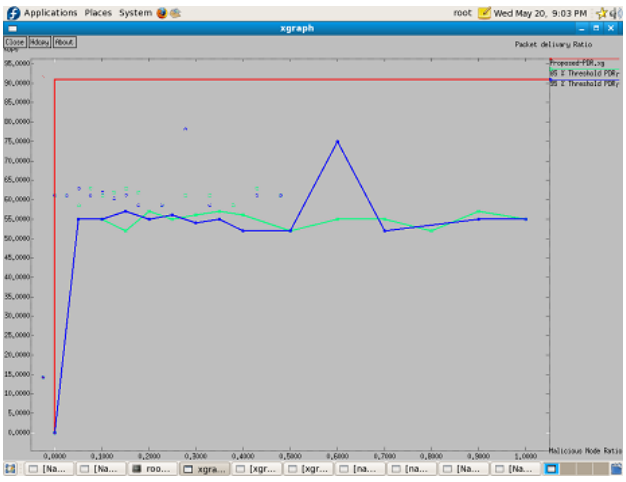

Fig. 2. Packet Delivery Ratio

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

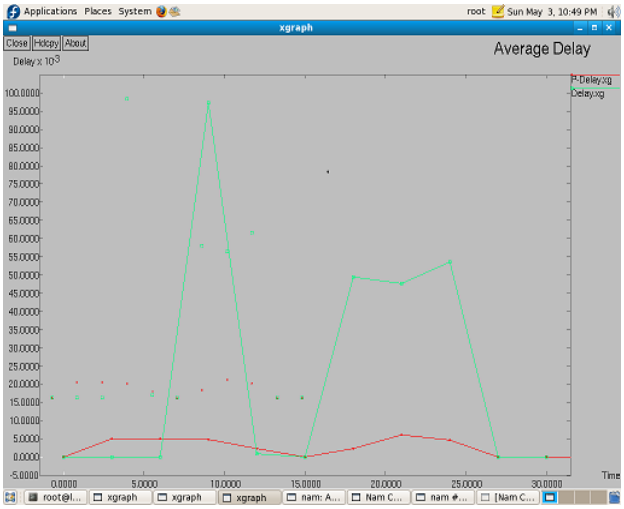

Fig.3. Average Delay

VI. CONCLUSION AND FUTURE WORK

The proposed work will probably detect the malicious nodes in the route, and as any malicious node is not participating in any route discovery the communication will be attack free. Also, the proposed methodology provides multipath to destination. So the shortest path to destination can be utilized. Moreover, as there is no Route Reply required and hence there is no backtracking, the time required for the route discovery will be less. Ultimately, proposed methodology detects malicious nodes, maintains blacklist of such nodes, finds multipath to destination and decrease the route discovery time.

REFERENCES

[1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai," Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach" IEEE SYSTEMS JOURNAL1932-8184 © 2014 IEEE.

[2] Dr. N. Sreenath, A. Amuthan, & P. Selvigirija "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs", International Conference on Computer Communication and Informatics (*ICCCI* -2012), pp. 1-7, 2012.

[3] K. S. Sujatha, Vydeki Dharmar, R. S. Bhuvaneswaran "Design of Genetic Algorithm based IDS for MANET", International Conference on Recent Trends in Information Technology (ICRTIT), pp. 28-33, 2012.

[4] Dr Karim Konate, Gaye Abdourahime "Attacks Analysis in mobile ad hoc networks: Modeling and Simulation", 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, pp. 367 – 372, 2011.

[5] Gandhewar, N., Patel, R. "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 714 – 718, 2012.

[6] Gajendra Singh, Amrita Gayakwad," Wormhole Detection and Prevention using Profile base Mechanism in MANET"International Journal of Computer Applications (0975 – 8887) Volume 95– No.7, June 2014.

[7] Ramanpreet Kaur, Anantdeep Kaur," Blackhole Detection In Manets Using Artificial Neural Networks "International Journal For Technological Research In Engineering Volume 1, Issue 9, May-2014

[8] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi, Sanjay K. Dhurandher "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks", proceedings of IEEE Global Telecommunications Conference (GLOBECOM 2011), pp. 1-5, 2011.