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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Eradication of Selfish Node in MANET Using CSNA Mechanism

P.Vijayalakshmi[1], P.Visvanathan[2]

PG Scholar, Dept. of CSE., Ganadipathy Tulsi's Jain Engineering College., Vellore, Tamil Nadu, India.

Assistant Professor, Dept. of CSE, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamil Nadu, India.

ABSTRACT: A Mobile unintentional Network could be an assortment of mobile nodes that communicate with alternative one another via wireless links either directly or indirectly betting on other nodes, because the nodes in MANETs are liberated to move at random, topology of a MANETs would possibly change quickly and unpredictably. The malicious nodes might cause security issues like gray hole and cooperative black hole attacks. To resolve these attack issue planning DSR routing mechanism. In our theme, the address of associate degree adjacent node is employed as bait destination address to bait malicious nodes to send a route reply RREP message, and malicious nodes are detected employing a reverse tracing technique. Localization of malicious nodes is often projected. This may increase the performance. The method describes transmission of information from one node to a different in secured manner together with localization.

KEYWORDS: DSR, MANET, Malicious node

I. INTRODUCTION

Communication is that the method by that two or additional individuals exchange their ideas or feelings. Types of networks available for communications today are Wired and Wireless networks [4]. An Adhoc network conjointly referred to as infrastructure less networks is advanced distributed systems comprises wireless links between the nodes and every node conjointly works as a router to forwards the information on behalf of different nodes. Unintended networks primarily have two forms, one is static unintended networks (SANET) and also the different one is named mobile unintended networks.

Some of the applications of MANETs square measure Military or police exercises, Disaster relief operations, Mine website operations, imperative Business conferences, mechanism knowledge acquisition. This often primarily owes to their infrastructure less property. Fig.1 describes the various applications of Manet. Unintended networks offer a prospect of making a network in things wherever creating the infrastructure would be not possible or prohibitively high ticket. In contrast to a network with fastened infrastructure, mobile nodes in unintended networks don't communicate via access points (fixed structures). Every mobile node acts as a bunch once requesting/providing information from/to different nodes within the network, and acts as router once discovering and maintaining routes for different nodes within the network [6].

However a node could misdemeanor by agreeing to forward packets thus failing to try and do so as a result of it's over laden, stingy or malicious or broken. A malicious node propels a denial of service attack by dropping packets.

Security in Mobile Ad-Hoc Network is that the most significant concern for the fundamental practicality of network. The availability of network services, confidentiality and integrity of the information may be achieved by reassuring that security problems are met. MANETs usually suffer from security attacks owing to its options like open medium, dynamic its topology dynamically, lack of central observance and management. These factors have modified the battle field scenario for the MANETs against the safety threats [4].

The MANETs work with a non-centralized administration wherever the nodes communicate with one another on the idea of mutual trust. This characteristic makes MANETs additional at risk of be exploited by associate wrongdoer within the network. Wireless links conjointly makes the MANETs additional vulnerable to attacks, that creates it easier for the wrongdoer to travel within the network and find access to the continuing communication.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

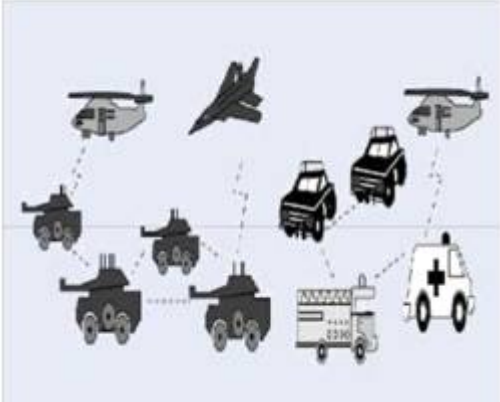

Fig 1. Manet Application

Mobile nodes present within the vary of wireless link will catch and even participate within the network. MANETs should have a secure manner for transmission and communication and this is often a quite difficult and important issue as there's increasing threats of attack on the Mobile Networks [7]. Security is that the cry of the day.

Preventing or detective work in malicious nodes launching gray hole or cooperative part attacks or the other attacks could be a challenge.

In region (black hole) attack, a malicious node uses its routing protocol so as to advertise itself for having the shortest path to the destination node or to the packet it needs to intercept [2]. This hostile node advertises its handiness of contemporary routes no matter checking its routing table. During this approach assaulter node can continually have the provision in replying to the route request and therefore intercept the information packet and retain it [9].

In gray hole attack the assaulter misleads the network by agreeing to forward the packets within the network. As shortly because it receives the packets from the neighboring node, the assaulter drop the packets. This can be a kind of active attack. At the starting the assaulter nodes behaves unremarkably and route reply true RREP messages to the nodes that started RREQ messages. Once it receives the packets it starts dropping the packets and propels Denial of Service attack. The malicious behavior of gray hole attack is completely different in numerous ways that it drops packets while forwarding them within the network [10]. It drops packets while forwarding them within the network. In another gray hole attacks the wrongdoer node behaves maliciously for the time till the packets are born so switch to their traditional behavior. In gray hole attacks, the malicious node isn't able to recognized intrinsically since it turns malicious only at a later time, preventing a trust-based security answer from detection its presence within the network. It then by selection discards/forwards the info packets once packets undergo it. Due to this behavior its terribly trouble some for the network to work out such quite attack. Gray hole attack is additionally termed as node misbehaving attack.

In this paper, our focus is on detective work on gray hole/collaborative black hole attacks by employing a dynamic source routing (DSR)-based routing technique. We have a tendency to conjointly perform the localization of the mobile nodes.

This paper describes a DSR routing mechanism that aims at investigation and preventing malicious node attacks. The benefit of DSR routing mechanism lies within the undeniable fact that it integrates the proactive and reactive defense architectures to attain the aforesaid goal. The precise position of the malicious nodes will be conjointly situated employing a beacon generator. By this we are able to forestall the more forwarding of packets through that path.

II. DSR ROUTING MECHANISM

Dynamic source Routing (DSR) may be a routing protocol for wireless mesh networks. It's the same as AODV therein it forms a route on-demand once a transmittal node requests one. However, it uses supply routing rather than looking forward to the routing table at every intermediate device. DSR protocol adapts quickly to routing changes once host movement is frequent, however needs very little or no overhead during times within which hosts move less oft.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

DSR involves two main processes: route discovery and route maintenance. To execute the route discovery section, the supply node broadcasts a Route Request (RREQ) packet through the network. If Associate in nursing intermediate node has routing data to the destination in its route cache, it'll reply with a RREP to the supply node [5]. Once the RREQ is forwarded to a node, the node adds its address data into the route record within the RREQ packet. Once destination receives the RREQ, it will grasp every negotiator node address among the route. The destination node depends on the collected routing data among the packets so as to send a route reply message to the supply node alongside the full routing data of the established route. DSR doesn't have any detection mechanism; however the supply node will get all route data regarding the nodes on the route. In our approach, we have a tendency to build use of this feature.

III. PROPOSED METHOD

In this mechanism conferred that effectively detects the malicious nodes that decide to launch gray hole/collaborative black hole attacks. In our theme, the address of an adjacent node is employed as bait destination address to bait malicious nodes to send a route reply message, and malicious nodes are detected employing a reverse tracing technique. Any detected malicious node is unbroken in an exceedingly region list so all different nodes that participate to the routing of the message are alerted to prevent human activity with any node in this list. It's supported a hybrid primarily based technique [6].

A. Phase Setup

The goal of the bait part is to provoke a malicious node to send a route reply by sending the bait RREQ that it's wont to advertise itself as having the shortest path to the node that detains the packets that were in demand. The supply node stochastically selects an adjacent node, inside its one-hop neighborhood nodes and collaborates with this node by getting its address because the destination address of the bait RREQ. Since every baiting is finished stochastically and therefore the adjacent node would be modified if the node affected, the bait wouldn't stay unchanged.

The malicious node can send a fate RREP for this RREQ stating that it'll be the shortest path to the destination. Therefore the supply node will simply establish that it'll be the malicious node.

B. Reverse Tracing Program

The reverse tracing program is employed to find the behaviors of malicious nodes through the route reply to the RREQ message. If a malicious node received a RREQ it will reply with a false RREP consequently, the reverse tracing operation are going to be conducted for nodes receiving the RREP, with the goal to deduce the dubious path data and also the briefly trusty zone within the route.

C. Localization

Localization of malicious node may be performed with the assistance of beacon generator. Base station can send beacon signal (hello message) with in an exceedingly range. The nodes present during this range can update its position with relevance x and y axis will send reply to the bottom station. Therefore the particular position of malicious node may be updated and also the forwarding of packets through this could be prevented.

A beacon may be a node responsive to its location.The nodes of at the start unknown positions are known as unknown nodes. When the sensing element node has been deployed, the mobile beacon assists the position unidentified nodes to localize themselves. The precision of the localization will increase with the amount of beacons. The many limitation associate with increased range of beacons is that they are costlier than the remainder of the device nodes.

IV.PERFORMANCE ANALYSIS

We think about the performance metrics of Energy and Throughput. The energy and throughput of the projected system is compared with existing technique. The results area unit showed in X graph.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A. Energy Parameter

The energy utilization of both the proposed and existing is examined. The graph representing this is given below.

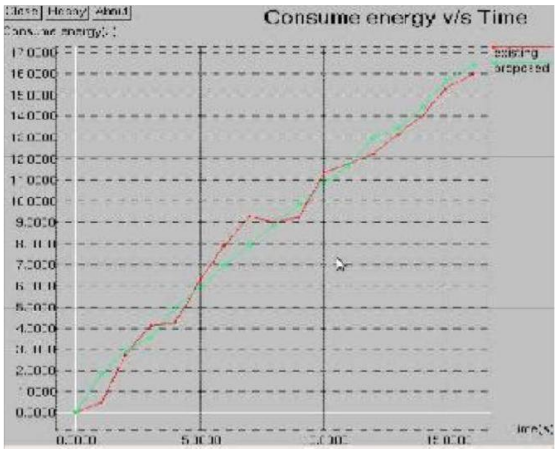

Fig 2. Energy Analysis

Here from above Fig 2. Explains that it is clear that our proposed technique saves energy than the existing technique saves energy than the existing.

B. Throughput Analysis

Next let us see the throughput graph of proposed versus existing. Proposed system provides a high efficient throughput than the Existing technique.

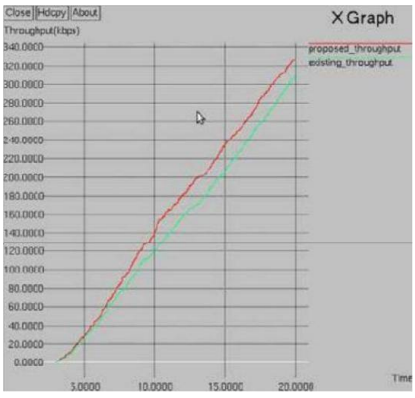

Fig 3. Throughput Analysis

Proposed system provides a high efficient throughput than the Existing technique. This is defined by the ratio of the total amount of data (*bi*) that the destination accepts them from the source and to the time (*ti*) it takes for the destination to get the last packet. The throughput measured by the number of bits transmitted per second. The throughput of the application traffic *n*, which is

$$T = \frac{1}{n}\sum \frac{bi}{ti} \quad (1)$$

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

V. CONCLUSION

In this paper the routing security problems with MANETs, are mentioned. Varied attacks caused by malicious node are represented. Cooperative Bait Detection theme with DSR routing is planned. . Malicious nodes present within the configuration are known. The attacks caused by these malicious nodes are additionally prevented. The share of packets received through the planned technique is great. The planned system additionally possess high turnout than the present technique. The planned system has achieved the most objectives expressed earlier. This is often an efficient mechanism to avoid the malicious node attacks. Localization of malicious node is planned. This technique can increase the network performance. The proposed method describes the transmission of knowledge from one node to a different in secured manner on with localization.

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 Journal 2014
2. A. Baadache and A. Belmehdi "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci.Inf. Security 2010
3. Chobe C.N. Deepali Gothawal "an Acknowledgement Based Approach For Routing Misbehavior Detection in Manet with AODV" International Journal of Advanced Computational Engineering and Networking 2013
4. Daniele Puccineli and Martin Haenggi, "WirelessSensor Networks: Applications and Challenges of Ubiquitious Sensing 2007
5. David B. Johnson, David A. Maltz, "Dynamic Source Routing in Ad Hoc Networks" Computer Science Department Carnegie Mellon University 1996
6. James parker, Jeffery Undercoffer, John Pinkston, and Anupam Joshi, "On Intrusion Detection and Response for Mobile Ad Hoc Networks" IEEE Systems 2009
7. Lidong Zhou and Zygmunt J. Haas "Securing Ad Hoc Networks" IEEE Journal 1999
8. Marti S, T.J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in Mobile Ad hic networks." Proc, 6th Annu. Intl. Conf. Mobicom, 2009
9. Ramaswamy.S, H. Fu, Sreekantaradhya M, Dixon J, and Nygard .J "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in proc, Int. Conf. Wireless network 2003
10. Senthilkumar Subramaniyan, William Johnson, Karthikeyan subramanian "A Distributed Framework for detecting selfish node MANET using Record and Trust-Based Detection(RTPD) technique" 2014
11. Reena Sahoo, Dr.P.M.Khilar "Detecting Malicious Node in MANET based on a Cooperative Approch" 2011
12. Min Liu, Ying Li "Load Balancing Mechanism and Selfish Nodes Detection in Peer-to-Peer Network" 2013

BIOGRAPHY

Vijayalakshmi.P is a PG Scholar in the Computer Science Department, Ganadipathy Tulsi's Jain Engineering College, Vellore. She received a B.E (CSE) degree in 2014 from under Anna University, P.T. Lee Chengalvaraya Naicker College of Engineering and Technology., Kancheepuram. Her research interests are MANET, Computer Networks, Neural Networks, Cloud Computing etc.

Visvanathan.P is Assistant Professor in Computer Science and Engineering Department in Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamil Nadu, India.