Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.369 – 374

RESEARCH ARTICLE

Acknowledgement Based Multipath Routing Scheme For Detecting Mallicious Nodes In MANET

[1]Miss. Neha B. Bhoyar
(M.E. 2nd Year, Computer Science & Engineering)
Department of Computer Science & Engineering,
G.H. Raisoni College of Engineering & Management, Amravati, Maharashtra
bhoyarneha333@gmail.com

[2]Prof. Poonam P. Borkar
Assistant Professor G.H. Raisoni, Amt.
Department of Computer Science & Engineering,
G.H. Raisoni College of Engineering & Management, Amravati, Maharashtra
poonam.borkar@raisoni.net

Abstract— Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station or a wired backbone network. MANET nodes are typically distinguished by their limited power, processing, and memory resources as well as high degree of mobility. In such networks, the wireless mobile nodes may dynamically enter the network as well as leave the network. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network. Thus routing is a crucial issue to the design of a MANET. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby a wireless local area network will form. 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, and leads 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. And the propose work implemented in NS2.

Keywords: ***ABRD, DSR, ACK status, ACKW packet, etc.***

I. INTRODUCTION

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 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 selfconfigurable 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.

There are five major security goals that maintain a reliable and secure ad-hoc network environment. They are

1] confidentiality,
2] integrity,
3] availability,
4] authentication and
5] non-repudiation.

Attacks in MANETs can be classified into two main categories: passive attacks and active attacks. Different types of passive attacks are: eavesdropping, location disclosure and traffic analysis. Active attacks include sleep deprivation, warmhole attack, blackhole attack, sinkhole, greyhole, rushing attack, Sybil attack and DDoS attack.

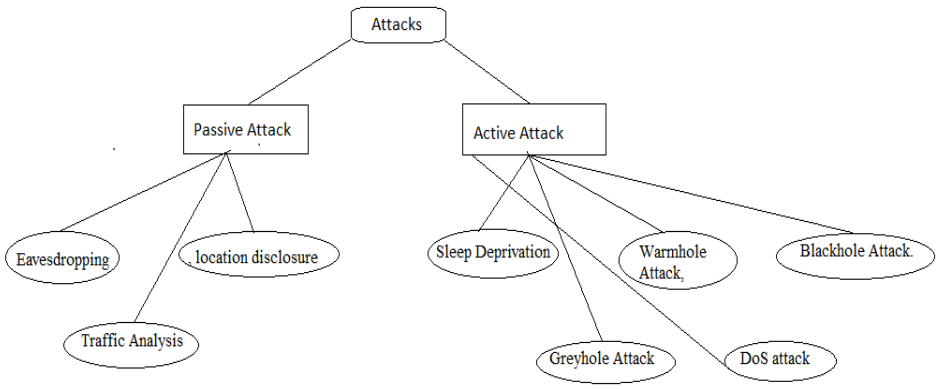

Fig.1: Classification Of Attacks in MANET

Mobile ad hoc networks (MANETs) are one of the fastest growing areas of research. A MANET is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predetermined organization of available links. Some characteristics of MANETs such as communication via wireless links, resource constraints (such as bandwidth and battery power), cooperation between the nodes due to communication protocols and dynamic topologies make it more vulnerable to attacks. Black hole attack is a wellknown security threat in mobile ad hoc networks. A black hole attack node attracts all packets by falsely claiming a fresh route to the destination node and absorbs them without forwarding them to destination. In recent years, different approaches have been implemented to improve the security of MANETs.

There are several applications of ad hoc network which need highly protected communication. Common applications of MANET are: military networks, business operations such as oil drilling platforms and emergency response operation such as after natural disaster such as a flood and earthquakes etc.

There are three types of routing protocols:

1] Reactive routing protocol,
2] Proactive routing protocol, and
3] Hybrid routing protocol.

The proactive routing protocols, sometimes called as table-driven routing protocol. In which each node continuously maintains up-to-date routing information to every other node in the network. Routing information is passed throughout the network in order to organise routing table continuously. Proactive protocols suffer from additional control traffic so that it wants to continually update the routing information. The network topology is dynamic, so that when a link goes down, each and every paths that uses that link are broken and that all have to be repaired. When a single application is not using these paths, then the effort which is being to repair may be considered wasted.

In contrast to proactive routing protocols, the reactive routing protocols sometimes called as on demand routing protocols, in which a node performs a route discovery throughout the network, only when it wants to send packets from source to its destination. This process is completed once a route is determined or all possible permutations are examined. After a route discovery, route is handled by a route maintenance phase until either the destination becomes inaccessible along every path from the source or until the route is no required for long time. In reactive detection mechanism scheme, nodes maintain the routes to active destinations. A route discovery is needed for each and every unknown destination.

In hybrid protocols, each node maintains both the topology information within its zone and the information regarding neighboring zones that means proactive behavior within a zone and reactive behavior among zones.

II. LITERATURE REVIEW

Chin-Feng Lai, Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao[1], these author propose "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach". In this the author discover a Dynamic Source Routing (DSR) mechanism which is also known as Cooperative Bait Detection Scheme (CBDS) for solving the problems of black hole and gray hole attacks which is caused by malicious nodes. In CBDA both proactive and reactive detection schemes are used to detect malicious nodes. A proactive detection scheme constantly detect the nearby nodes and avoid attacks in its initial stage. In reactive detection scheme it triggers only when detection node detects any significant drop in packet delivery ratio. By using Reverse tracing technique it achieve its goal. Cooperative Bait Detection scheme is proposed to detect malicious nodes in Manet for the gray hole and black hole attacks.

Jing-Wei Huang, Isaac W., Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi, S. K. Dhurandher [3] proposed A Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks. This work uses a trust based multiple path routing i.e AOMDV which is combined with soft encryption method, which is sometime called as T-AOMDV scheme. This approach consists of following three steps:

(1) The first step is Message encryption, in which the message is segmented into three parts. And these three parts are encrypted by one after another by using some XOR operations,

(2) Then in second step i.e Message routing, the message parts are passed through different trust based multiple paths using a novel node disjoint a protocol AOMDV &

(3) Finally In last step i.e Message decryption, the destination node decrypts the message for getting the original message.

Dr. N. Sreenath, A. Amuthan, & P. Selvigirija [4], proposed Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs. This work aims to improve the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) against the flooding as well as black hole attacks. The proposed mechanism is implemented for flooding attack. And it works when the identity of the

malicious nodes is unknown for this purpose there is no require any additional network bandwidth. The performance of a small group will degrade seriously under these types of attacks even the solution is available.

K. S. Sujatha, V. Dharmar, R. S. Bhuvaneswaran [5], proposed Genetic Algorithm based IDS for MANET. In this work a technique is used to analyse the attacks in AODV, specifically in the most common network layer hazard which is most common, as well as attacks like Black Hole attack. Author develop a specification based Intrusion Detection System (IDS) using Genetic Algorithm approach. In proposed system to analyses the behaviours of each and every node Genetic Algorithm is used. And the algorithm provides details about the attack. The propose system introduce (GAC) that is Genetic Algorithm Control. GAC is a set of number of rules based on the various features of AODV such as Forwarding Request Rate, Rate of Reply Receive & so on.

Dr Karim Konate, Gaye Abdourahime [6], proposed an Attacks Analysis in mobile ad hoc networks: Modelling and Simulation. In this title the author presents a work which is dedicated to study of various type of attacks in MANET. They introduce several alternatives for DOS attacks that is Denial of service attacks in MANETs.

Gandhewar, N., Patel, R [7], proposed Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Ad-hoc Network. The propose work mainly focuses on sinkhole problem, & presents a mechanism for detection & prevention of it.

Gajendra Singh and Amrita Gayakwad [8] propose An Approach to Defend against Wormhole Attack in Ad Hoc Network Using Digital Signature. The author present a mechanism which is helpful in prevention of wormhole attack in ad hoc network is verification of digital 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 the attack which is formed by two malicious nodes and a tunnel. The author used a scheme to protect from wormhole attack, called as multi hop count analysis (MHA) with verification of legitimate nodes in network through its digital signature.

III. MOTIVATION

Sometimes in the routing the malicious nodes are detected. For that purpose many routing scheme are detected but the time required to detect the malicious node and after that again the path discovery from source to destination are much more time consuming and also the routing overhead is increase in the transmission of packets.

So these basic problems in the routing must be overcome to reduce time complexity and routing overhead I will try to develop the multipath routing concept related to CBDS scheme.

IV. PROBLEM DEFINITION

In a normal AODV route discovery process. For example, if the node S starts a route discovery process by broadcasting a RREQ message, then all the neighbours of S will receive the request and process the request. If a neighbouring node knows the route, then it will send a reply otherwise, it will forward the RREQ message by re-broadcasting it again. In fact, all the nodes in the network will receive that RREQ message. If the message will reach the destination D, then D will send a RREP message.

Based on above discussion, it is noticed that most of the above mentioned protocols is applicable in multipoint MANET and all of them tries to minimize the number of messages. However, to achieve this it is observed that lot of energy is consumed or special hardware is required. Thus, it is imperative that a protocol is required to reduce the number of messages during broadcasting to avoid flooding.

V. OBJECTIVE

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.

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.

In the above process if any ACKW packet which does not contain a route from source to destination in end-to-end delay time, then, such packets is discarded and the FN node specified in last ACK status will added to blacklist. From the entire valid ACKW packet shortest route can be utilize for further communication.

VI. PROPOSED WORK

This work uses Dynamic Source Routing for route discovery. DSR involves two main processes: route discovery and route maintenance. Our approach has three main factors:

1. RREQ packet- Contains Generation time stamp, Source node address, Destination Address and Intermediate Node Address [1], Intermediate Node Address [2] Intermediate Node Address [n].
2. ACK status i.e. Acknowledgement from node participating in route discovery. It contains the address of node which receive the RREQ packet and address of node to which it forwarded the RREQ packet. Receiving Node will be called as RN and Forwarded Node will be called as FN.
3. ACKW packet- keeping the track/route of ACK status for each neighbor or intermediate node.

To execute the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the network. On first hop RREQ packet is accepted by all neighbour node. Each neighbour will transmit it to their intermediate node and at the same time will send an ACK to source node. At source ACKW packet receive ACK for a particular neighbours as there will be ACKW packet same as in numbers of source's neighbours. Each ACKW packet will accept the ACK from intermediate node and path will be discovered to destination. Here there is no need of Route Reply (RREP)

VII. MODULES

In proposed work up till, we are at now two modules. They are as follows

1] Neighbour finding

2] Transmission of Packets

VII.1 Neighbor finding

In the first module, Network topology is formed so that each node finds its neighbouring node. As shown in Fig.6 (a). Each node send topology packet in network and form a Network Topology. This work is done in network simulator 2.

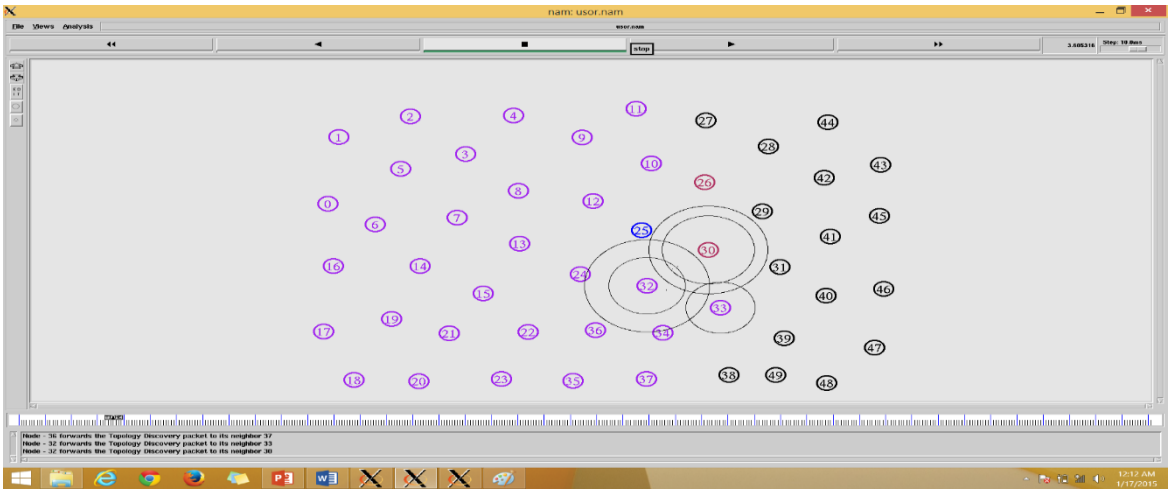

Figure 6(a): Snapshot of Neighbour finding

VII.2 Transmission of Packets

In the Transmission of packets, after finding the neighbour and forming a network topology, packet transmission is done shown in fig.6 (b). Here we are considering source node as 0 and destination as 9. So that source node send the RREQ pkt. to its neighbouring node and each neighbouring node send the ACK to source node and at a same time receiving node forward RREQ to its neighbouring node. This process will done until pkt. reaches at destination.

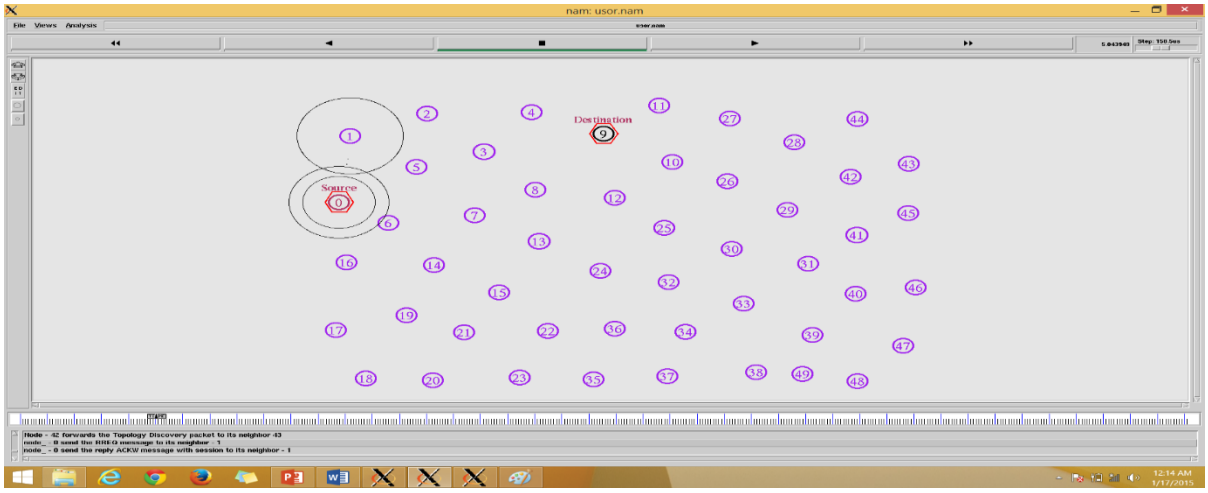

Figure 6(b): Snapshot of Transmission of Packets

VIII Conclusion

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. Till now we are successfully implemented the two module of the proposed system.

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 1932-8184 © 2014 IEEE.

[2] 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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[10] Hamid Al-Hamadi and Ing-Ray Chen," Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks" IEEE Transactions On Network And Service Management, Vol. 10, No. 2, June 2013

