IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735
PP 08-14
www.iosrjournals.org

Misbehavior Detection and Elimination of Rely node in Wireless Ad-hoc Networks using Candidate Elimination Algorithm

[1]Gowthamraj, [2]M.Citharthan(Assistant Professor),
[1,2]Department Of Electronics And Communication Engineering,
Sri Krishna Engineering College, Anna University,
Chennai, India.

Abstract- *Mobile Ad Hoc Network (MANET) is formed by a set of wireless mobile hosts that dynamically configure themselves by exploiting their wireless network interfaces without relying on any fixed infrastructure. This is a challenging task for the mobile hosts that have limited resources such as processing power, storage and energy. Misbehavior is defined as an unauthorized behavior of an internal node that results unintentional damage to other nodes. For instance, one may not correctly execute the MAC protocol with the intent of getting higher bandwidth or it may refuse to forward packets for others to save its resources, while using their resources and asking them to forward its own packets. This paper present a candidate elimination algorithm to detect the malicious attack using per hop distance and pixel wise measurements link frequent appearance count parameters using AODV. The simulation results of the proposed scheme shows a promising result in the measured parameters when compared to the existing scheme. Candidate elimination algorithm is used to eliminate the misbehaving node in MANET.*

Keywords- *Wireless Ad-hoc Networks, Candidate Elimination Algorithm*

I. INTRODUCTION

Mobile Adhoc Network (MANET) is referred to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily. MANET is one of the most important and unique application used for the industrial purposes. It is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. It does not require a fixed network infrastructure. It can be subdivided into two types. In single hop networks the nodes are within communication range can communicate directly with each other. In Multi-hop networks, if the nodes are out of communicating range, the nodes must rely on intermediate nodes to forward the data packets to their destination. However, in both type of networks there is no dedicated link available like the links in wired networks. The absence of fixed and dedicated link among the nodes leads to severe security threats to the network.

MANET are susceptible to having their effective output compromised by variety of security attacks because of features like unreliability, constantly changing topology, restricted battery power, lack of centralized control and others. Nodes may misbehave either because they are malicious and deliberately wish to disturb the network or because they are selfish and wish to conserve their own limited resources such as power.

Types of MANETS:

- In a closed MANET, all mobile nodes cooperate with each other towards a common goal, such as emergency search/rescue or military and law enforcement operations.
- In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity.

For instance, battery power is considered to be most important in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish nodes or misbehaving nodes and their behavior is termed as selfishness or misbehavior participates. One of the major sources of energy consumption in the mobile nodes of MANETs is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

II. ATTACKS ON MANET

Eavesdropping: The simplest attack on a wireless net is eavesdropping; it requires minimal preparation and cannot be detected. Eavesdropping can be subdivided as follows:

Non-Participation: After joining the MANET a node could simply refuse to forward other node's data (often called free riding).

Denial of Service: With enough resources an attacker can always send more data than other nodes can process. Mobile clients are especially vulnerable to denial of service attacks because it quickly drains their energy reserve. Another possible approach does not even need to send large amounts of data but just sending enough packets to prevent a node from going into sleep-order energy saving-mode; this is called sleep deprivation.

Simple denial of service – some routing protocols allow very simple attacks, like sending data for non-existing targets, thus creating a route-finding broadcast.

Black hole – a node can announce itself as having the shortest path to all other nodes, thus it disrupts existing routes and attracts much traffic. Getting a large amount of data leads to new opportunities like selectively forwarding or dropping packets or various kinds of traffic and content analysis.

Wormhole – collaborating attackers can create two or more black holes and connect them (out of band, e. g. by directional antennae or wire). This gives them control over large parts of the MANET and its packets.

Sybil attack – a single malicious node can simulate a number of independent nodes. This is basis for a lot of manipulations: it favors the client in bandwidth allocation, gives influence on routing decisions, and undermines every kind of voting algorithm or threshold cryptography.

III. SYSTEM ARCHITECTURE

Manet Aodv Architecture

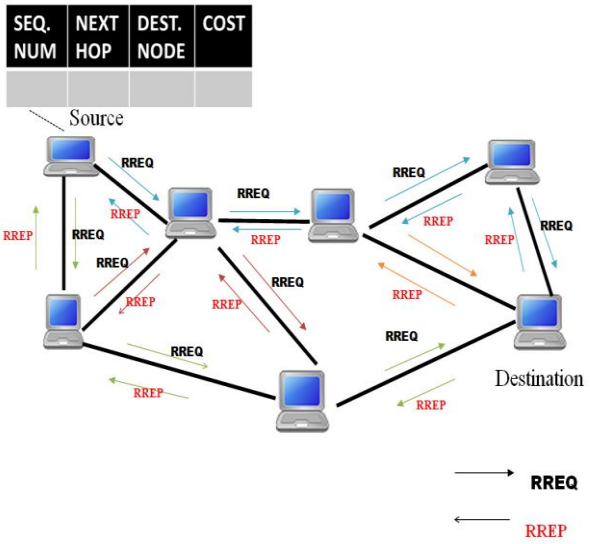

Fig 1.MANET AODV ARCHITECTURE

The MANET AODV architecture diagram shows the network formed between the source and destination nodes. It shows the request and reply of the source and destination nodes. It helps the source node to find the shortest path on the network. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. AODV is, as the name indicates, a distance-vector routing protocol.

ARCHITECTURE DIAGRAM

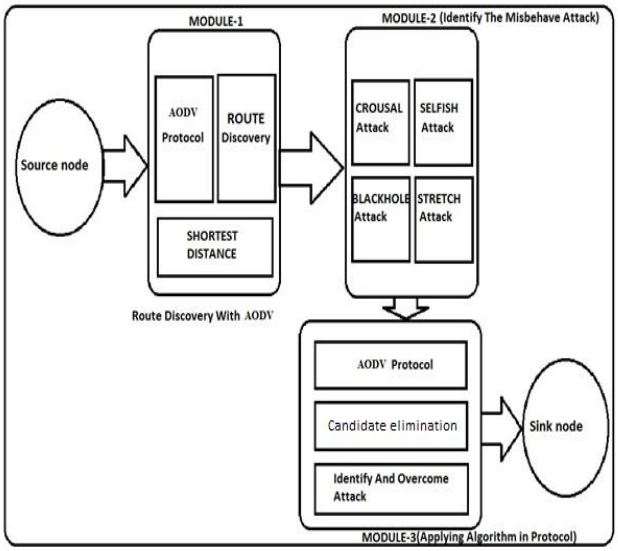

Fig 2.ARCHITECTURE DIAGRAM

In this Architecture diagram the three modules are used to do the operation in detection and elimination of the misbehaving nodes in MANET

The modules are present between the source and destination nodes. The first module is used for ROUTE discovery, the second module is used to find the type of attack take place in network, and then the third node is used to eliminate the misbehaving node in the network.

IV. EXISTING APPROACH

An ad hoc network nature is the main cause for making it more Vulnerable to wireless attacks. Ad hoc nodes are wireless in nature that makes it Prone. Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge.

- Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic so it's making data transmission problem.
- When we sending our data to destination in the techniques will not give more security, we don't know the accurate selfish node in our infrastructure Ad-hoc network so in this also main drawback of our wireless Network.
- Another Problem it will drop more dropping packets, making time delay, reduce delivery ratio, as well as throughput because of selfish node.

V. PROPOSED APPROACH

Mobile ad hoc networks (MANET) rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. Detecting routes and forwarding packets consumes local CPU time, memory, network-bandwidth, and last but not least energy. Here we implementing and finding the dropping packets for optimal estimation for using candidate elimination algorithm in AODV. We proposed candidate elimination algorithm to detect the malicious attack using per hop distance and link frequent appearance count parameters in AODV.

Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data. AODV protocol is vulnerable to numerous attacks from malicious, compromised and malicious nodes. Therefore, AODV demands **for special mechanisms to enhance its security.**

VI. MODULES

In this proposed system, we have many modules. They are given by,

AODV Route Discovery

In first module we go to identify the route at very shortest distance by using the AODV protocol. AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates. AODV is capable of both unicast and multicast In AODV, the network is silent until a

connection is needed. At that point the network node that needs a connection broadcasts a request for connection.

Identify the Attacks

In normal data transfer, we go to identify the hacker nodes and also malicious node. Malicious node is create the some major problems like packets drop, delay time, low delivery ratio, and also packet loss. This problem occurs when data transfer from source to destination.

Packet Dropper in Manet

A secured MANET system can be achieved only by preventing routing protocol attacks. The malicious is one of the challenging attacks in the ad hoc routing in which two malicious nodes forms a tunnel with high transmission connectivity referred as a malicious tunnel. The malicious tunnel may be wired or wireless form or an optical link. As soon as malicious nodes launch a malicious link they start gathering the wireless data and forward it to one another. It is then relay the packets over the malicious tunnel to some other location.

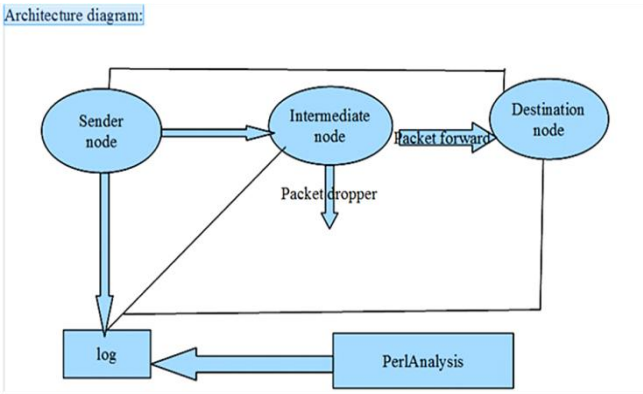

Fig 3.PACKET DROPPER ARCHITECTURE

The legitimate data packets are relayed to some other place in the network and malicious nodes makes other nodes to believe that they are immediate neighbors. The malicious attack affects both the proactive and on demand routing protocols. In this project AODV Protocol is used to analyze its behavior in MANET while sending packet and receiving packet to identify using path tracing algorithm.

PER HOP ESTIMATION

The presence of malicious can be detected by calculating the distance between each hop in a path. We consider round trip time (RTT) value to calculate the per hop distance. RTT is defined as RREQ and RREP propagation time between the source and destination. Let us consider the RTT calculation between two nodes A and B where both the nodes are non-packet dropper nodes.

IMPLEMENTING CANDIDATE ELIMINATION ALGORITHM

We have to successfully implementing the CANDIDATE ELIMINATION ALGORITHM in this project. The main function of path tracing algorithm is used to identify the hacker node and also malicious node in this network. It increase the data transmission speed, less delay, more efficiency, less packets loss, increase the packets delivery ratio.

ESTIMATION OF PACKET DELIVERY:

After detecting packet dropper node, we need to take accurate measurements for packet sending and reviving design an effective defense mechanism for malicious attack. To achieve the goal, we proposed to detect the malicious node using per hop distance and link frequent appearance count Parameters to develop the extension of AODV routing protocol.

VII. RESULT AND DISCUSSION

Create a wireless network using the front end language TCL. Set the network with 6 nodes which are dynamic in nature. Node 2 is made to move at time =3.4ms in defined direction. Node 5 is made to move at time =4.3ms in defined direction. At time = 2.5ms node 3 becomes hacker node and stops forwarding packets. At time = 3.0ms node 3 is back to normal and forwards packets. At time = 3.5ms node 1 becomes malicious node and stops forwarding packets.

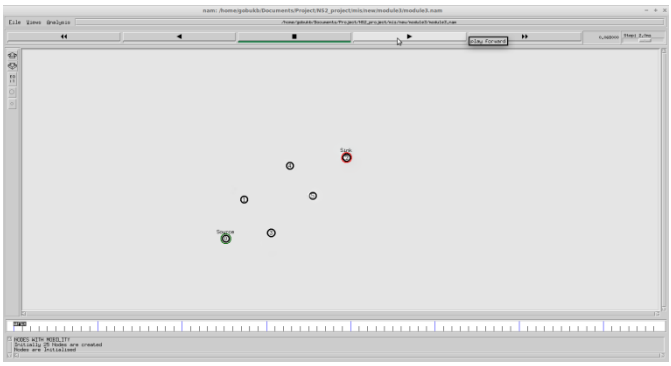

Fig 4.NAM FILE

At time = 5ms node 1 is back to normal and forwards packets. Malicious node is indicated by red color in the animator window .Malicious node is detected and prevented in the network using Path Tracing Algorithm.

The output is analyzed using trace file, log file and Perl analysis.

CANDIDATE ELIMINATION ALGORITHM

We have to successfully implementing the CANDIDATE ELIMINATION ALGORITHM in this project. The main function of path tracing algorithm is used to identify the hacker node and also malicious node in this network. It increase the data transmission speed, less delay, more efficiency, less packets loss, increase the packets delivery ratio.

Step to detect the malicious attacks.

Step 1: Nodes in a path computes RTT values based on the time between the RREQ sent and RREP received. The RTT computation is based on its own clock.

Step 2: Compute per hop distance value using RTT value. The computed per hop distance value and time stamp are stored in each packet header.

Step 3: These information are stored to identify the malicious link. Every node in a path computes per hop distance with its neighbor and compares it with the prior per hop distance. If the per hop distance exceeds the maximum threshold range, RTh, go to step 4.

Step 4: Check for the maximum count a link takes part in the path. If F Account > FATh, then the link is malicious.

Step 5: Mark the link as malicious and the corresponding node informs other nodes to alert the network. These malicious nodes are then isolated from the network.

Packet Delivery Ratio

PDR is the proportion of the total amount of packets reached the receiver and amount of packet sent by the source. If the amount of malicious node increases, PDR also decreases gradually. The higher mobility of nodes causes PDR to decrease. PDR = Total amount of data packet received (Destination) to the amount of packet sent (Source)

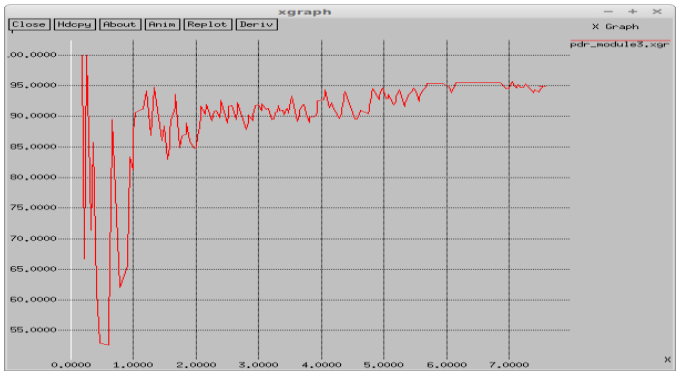

Fig 5.PACKET DELIVERY RATIO

THROUGHPUT

The throughput decreases as the amount of malicious nodes increase .The throughput of general DSR is 87% at the node mobility of 10 m/s for 10 malicious nodes and that of AODV is 95%. However the PT algorithm gives 97% of throughput.

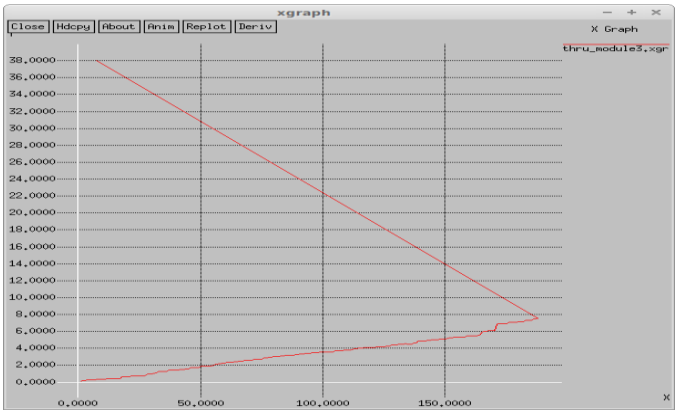

Fig 6.THROUGHPUT

AVERAGE DELAY

The average delay is the elapsed time between the packet sent and received

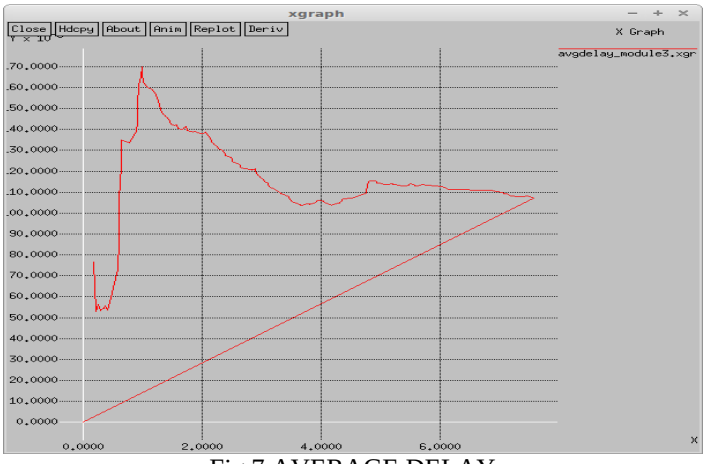

Fig 7.AVERAGE DELAY

VIII. CONCLUSION

In this reputation based scheme, built on top of normal AODV secure routing protocol the malicious attack which is one of the network layer attacks. This launches attacks by forming a tunnel between two or more malicious nodes and drops all the packets. To detect and prevent the malicious attack, we proposed CANDIDATE ELIMINATION (CE) algorithm. The CE algorithm to detects and prevents the malicious attack and eliminate the all malicious node using per hop distance between two nodes. From the simulation and analysis results, it is clear that our proposed algorithm is more effective in preventing the malicious attack with greater throughput and less average delay. The performance analysis addresses that CE algorithm has reduced overhead and delay. These results, along with advantage that no additional requirement of hardware makes the proposed system more suitable for resource constrained wireless network applications. Thus newly proposed reputation-based scheme, built on top of normal AODV secure routing protocol, achieves a higher throughput than the normal AODV in the presence of malicious nodes. Thus, the proposed design, Reputed-AODV, proves to be more efficient and more secure than normal AODV secure routing protocol in defending against both malicious and authenticated malicious nod.

REFERENCES

[1]. Abdalrazak T. Rahem, H K SAWANT "Collaborative Trust-based Secure Routing based Ad-hoc Routing Protocol "in International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.2, Mar-Apr 2012 pp-095-101

[2]. Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni "Improving Malicious Node Detection in MANETs Using a Collaborative Watchdog" in IEEE COMMUNICATIONS LETTERS, VOL. 16, NO. 5, MAY 2012

[3]. Ayday,.E Lee,.H and Fekri,.F(2010)"Trust Management and Adversary Detection for Delay-Tolerant Networks,"Proc. Military Comm.Conf.(Milcom '10).

[4]. Burgess,.J Gallagher,.B Jensen,.D and Levine,.B(2006) "Maxprop:Routing for Vehicle-Based Disruption-Tolerant Networks," Proc.IEEE INFOCOM '06.

[5]. Chen.B.B and Chan,.M.C "Mobicent(2010): A Credit-Based Incentive System for Disruption-Tolerant Network,"Proc. IEEE INFOCOM '10.

[6]. Douceur,.J (2001)"The Sybil Attack," Proc. Revised Papers from the First Int'l Workshop Peer-to-Peer Systems (IPTPS '01).

[7]. Fudenberg,.F.D and Tirole,.J(1991) Game Theory. MIT Press.

[8]. Gao.W and Cao,.G(2011) "User-Centric Data Dissemination in Disruption-Tolerant Networks," Proc. IEEE INFOCOM '11.

[9]. Hossmann,.T Spyropoulos,.T and Legendre,.F(2010) "Know the Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing," Proc. IEEE INFOCOM '10.

[10]. Keranen,.A Ott,.J and Karkkainen,.T(2009) "The ONE Simulator for DTN Protocol Evaluation," Proc. Second Int'l Conf.Simulation Tools and Techniques (SIMUTools '09).

[11]. Lindgren.A and Doria,.A(2007) "Probabilistic Routing Protocol for Intermittently Connected Networks,"draft-lindgren-dtnrg-prophet-03.

[12]. Li,.F Srinivasan,.A and Wu,.J(2009) "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets," Proc.IEEE INFOCOM '09.

[13]. Li,.Q Zhu,.S and Cao,.G(2010) "Routing in Socially Selfish Delay-Tolerant Networks," Proc. IEEE INFOCOM '10.