Detection of Non Consecutive Malicious Nodes Under Black Hole Attack In Manet

Harveen
Indo Global College of Engineering, Abhipur
Punjab Technical University, Jalandhar

Vanita singh
Asstt. Prof. Computer Science Dept.
Indo Global College of Engineering, Abhipur

Abstract- Mobile networks are very popular today. But on the other hand there are threats on mobile adhoc network. Black hole attack is one of the possible attack in Manet . Black hole attack is also called packet drop . A black hole attack has become a critical threat. Black hole attack affects the network performance. Gray hole attack is the attack in the network layer. The gray hole attack degrade the performance of network . The variation of black hole is gray hole attack. Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker. This attack is also known as routing misbehavior attack. The gray hole attack active attack .In the current work we have present the method to identify and removal of Non consecutive malicious node in Manet.

Keywords- Mobile Ad-hoc Networks, Black Holes, Routing, DSR, malicious, MANETs, attacks .

1. INTRODUCTION

Now -a-days, Mobile ad hoc network is one of the recent active fields. It has received more attention due to its self-configuration and self-maintenance properties . The Manet (mobile adhoc network) is defined as network which consists of mobile nodes. These mobile nodes are connected through wireless links. Here the mobile nodes means the devices like laptops, mobile etc. Adhoc is a latin word it means for this purpose. Every device in the Manet is free to independently move in any direction. Manet use wireless connections to connect to various networks. MANETs are restricted to a local area of wireless devices while others may be connected to the Internet. In Manet there are mobile nodes that form the temporary network . In the Manet there is no need any base station and wires so that it can be setup anywhere . In the Manet the nodes perform the roles of as server and client. The mobile adhoc networks are fully distributed. In the Manet the data must be pass through intermediate nodes. Manet are kind of wireless adhoc network that usually has a routable networking environment on the top of link layer ad hoc network, and these can change their positoin and configure itself on fly. Because of their changes in nature they are typically not very secure so it is important to be caution what data is sent over a manet. Each node in Manet operates not only as a host but also as act a router that forwarding packets to other mobile nodes in the network .It is not necessary that they are within the direct transmission range . Each node that is participates in an ad hoc routing protocol allows it to discover multi-hop paths through the network to any other node. Although mobile ad hoc networks have several advantages over the traditional wired networks, but on the other hand they have a unique set of challenges. Various types of attacks like *DoS* (Denial of Service) can easily be flood the network with spurious routing messages through a malicious node . These messages gives incorrect updating information by pretending to be a legitimate change of routing information. In manet an attacker can attempt to listen, modify all the traffic on the wireless communication channel as one of the legitimate node in the network.

A vanet is a type of Manet that allows the vehicle to

ISSN: 2278 – 1323

communicate with roadside equipment. But the vehicles may not have a direct connection of internet, the wireless roadside equipment may be connected to the internet allowing the data from the vehicle to be sent over the internet. Due to its varying nature MANET has larger security issues than conventional networks. AODV is a source initiated on-demand routing protocol. In the manet each mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. Manet face many challenges in the secure communication .

1.1 Characteristics

i) Manet require limited security .

ii) Mnaet can be set up anywhere.

iii)There is no need of any controller that is located in the centre. Means Each node in the manet perform its own functions. Each node is responsible for forward the data traffic .

iv)In Manet the every mobile nodes communicate by sending request and response message.

v) A node in manet uses the service discovery protocol so that it discover the service of its nearby node .

vi) In the manet any mobile node can node can participate in forwarding the data packets function .

1.2 **Applications of manet**

There are quite a number of uses for mobile ad-hoc networks.

***i)Urgent business Meeting*:** The persons of the company want to communicate or cooperate with the outside people so that they can share or exchange the information.

ii) Crisis management applications : The natural disaster that leads to the confused or disorganized whole communication. With the help of ad hoc network the whole communication infrastructure could be set up in small hours .

***iii) Personal area network and Bluetooth* : In** personal area network is a network it consists of nodes these nodes are associated with particular person's belt watch etc. Personal area networks typically involve a mobile computer, a cell phone and/or a handheld computing device such as a PDA. Bluetooth is a wireless technology. It for exchanging data over short distances. Bluetooth is a technology that support the pan by eliminating the need of wires.

Routing Attacks in Manet

1)Black Hole attack: This is kind of denial of service attack . The attacker advertises that the node has the shortest route to the destination node who is active on a compromised node in interested packet. According to that all the nodes of the network would adjust their routing table and send the packets to the particular node that drop or alter the packets called the compromised node.

2) Worm Hole attack: It is a network layer attack . It is the attack in Manet routing . In the warm hole attacker receive the packet at the one point and pass them it to the another point and reply them in to the that point in the network .

3) Partition attack: This attack makes false route advertisements in such way that the network is divided in to different sets, which either not reachable at all or reachable only through the attacker.

4) Gray hole attack : This is nown as routing misbehavior attack. The grey hole attack cause dropping of messages . There are two phases of grey hole attack . in the first phase the node advertises that it have the valid route to the destination . in the second phase the node drops the intercepted packets.

5)Malign attack: In this attack malicious nodes blackmails a true (good) node and spoils its reputation.

6) Jelly Fish attack: This is passive type of the attack. The jelly fish attack is difficult to identify.The jelly fish attack has following characterstics like

a) deliver all packets in scrambled order

b) selective black hole

c) hold packets that are received for a longer time.

7) Resource Consumption Attack: In this the attacker tries to consume the node's resources . These resources are battery power, computational resources, such as bandwidth, disk space, processor time. This is done by sending the forged route request packets to the nodes.

ISSN: 2278 – 1323

8) Route Invasion Attack: In the Route Invasion Attack the attacker sends Route request packets and tries to add itself to the route through which the source and destination are interested to communicate .

9) Rushing attack: In the rushing attack Route request are processed or forwarded without considering the Medium Access Control layer and routing protocol specifications, so that increasing its chance to be selected as an intermediate node in the route.

2.RELATED RESEARCH

1. In 2012" **Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs**", Gundeep Singh Bindra, Ashish Kapoor , Ashish Narang , Arjun Agrawal dscribed that Manet consists of nodes. These nodes are free to move. Different types of attacks like black hole and gray hole attack affect the infrastructure of manet. In this paper the author purposed a solution Purposed a solution of Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs . In this paper extended data routing information table is maintained at each node. In the DRI table it has through and from entries for other nodes.

2 . In 2012 "**Prime Product Number based Malicious Node Detection Scheme for MANET"** Sapna Gambhir , Saurabh Sharma purposed a method of Prime Product Number based Malicious Node Detection for MANETs. This method based on AODV. In PPN method every Cluster head (CH) node maintains the neighbor table which is used to keep information about all the nodes. In the modified protocol, the source node (SN) broadcasts a RREQ message to discover a secure route to the destination node. The intermediate node (IN) that generates the RREP has to provide information regarding its cluster head and product of all prime numbers from destination to source node in the form of Prime Product Number (PPN). Upon receiving the RREP message from IN, SN with the help of its cluster head (CH) will divide the PPN with the Node IDs to chec whether IN is its reliable node.

3.In 2012 "**Preventing Packet Dropping and Message Tampering Attacks on AODV-based Mobile Ad Hoc Networks"** Mohammad s. obadiat, Issac wounganag, sunjay kumar purposed a method that use the concept of that mock packets. The number of mock packets sent is obtained by dividing the payload size of the actual packet by 48. In order to obtain a reliable limit of tolerance, there needs to be sufficient number of cpkt and cmiss. Source calculates the ratio cmiss/cpkt to obtain the Limit of Tolerance. If this ratio is less than or equal to 0.2 then R is not discarded from the routing table and is deemed good. If the ratio is more than 0.2 R is considered to contain some malicious nodes. S discards the route R, adds the next hop from S to a blacklist and Route (R) is obtained through the regular AODV protocol.

4. In **2012 "Malicious AODV Implementation and Analysis of Routing Attacks in MANETs**" Humaira Ehsan Farrukh Aslam Khan describe that attacks against Manet named as black hole attack sinkhole attack selfish node behavior RREQ flood and selective forwarding attack by using the packet efficiency, routing overhead, and throughput as Performance metrics. This paper result shows that flooding attacks such as sinkhole and blackhole affect the packet efficiency and slow down the throughput. In this paper we examined that if the attacker node is on the path means if it is from source to destination then selfish node attacks can be very effective. It can cause of degrade the network performance.

5. In 2012 **"Effects of Malicious Attacks in Mobile Ad–hoc Networks"** Ashok M.Kanthe, Dina Simunic and Ramjee Prasad describe that Manet consists of mobile nodes .In the manet the mobile nodes have limited resources such as bandwidth and storage space. Manet become venerable for different types of attacks such as black hole attack gray hole attack etc. these are type of denial of service attacks. This paper shows that effects of black hole and gray hole attacks by using the different performance metrics like end toend delay and packet drop rate. This paper shows that if the number of melicious nodes increase it it degrade the performance of manet

ISSN: 2278 – 1323

6. In 2012 **"A Simulation Study of Malicious Activities under Various Scenarios in Mobile Ad hoc Networks (MANETs)**" Akshai Aggarwal Gujarat Technological University, and Nirbhay Chaubey described that manet play the important role in wireless communication . In this paper we study various security issues malicious node activity in AODV under different terms like network size traffic load which affect the packet delivery ratio end to end delay. Due to the unique nature and unique characterstics of MANETs, It creates a number of challenges to its security design.

7. In 2013 **"Black hole attack prevention in manet using route caching**" Prachee N. Patil and Ashish T. Bhole define a new approach for black hole prevention in DSR based on route caching.]Prachee N. Patil, Ashish T. Bhole purposed a new approach for blackhole prevention in DSR using the route cache mechanism of DSR. In this method first of all we have to get the blackhole node id. This is obtained during the path construction phase .Then we *add to path* function of DSR. In that function paths are ready to add in route cache, but priory to adding each path in route cache we are parsing only those paths for the presence of blackhole node id. If the blackhole node is appears in path, we have to simply dump that path and add all other paths for the source destination pair communication. This process uses of normal time of caching process only.In this Method delay is minimized as compared to previous blackhole detection mechanisms, packet dropped ratio is reduced drastically

8. **"Performance Evaluation Of Mobile Adhoc Network Under Black Hole "** Konagala pawani and Dr. Demodram avula purposed a method of performance evaluation of mobile adhoc network under black hole attack . This paper consider some parameters and evaluate the performance of Manet under black hole . In this paper they used the AODV as a routing protocol. It uses the metrics like PDR , Packet loss, Throughput. We conclude from this paper that throughput under the normal conditions increase as compared to the Manet under black hole packet loss of a network under the normal conditions is less than network under the black hole attack. Any network desire higher PDR. The PDR of the network under black hole attack is less than the network under black hole attack.

9. "**PPN prime Product Number Based Melicious Node Detection Scheme For Manet"** Sapna Gambhir , Saurabh Sharma purposed a method of Prime Product Number based Malicious Node Detection for MANETs. This method based on AODV . It can efficiently avoid malicious node attacks during path setup between source and destination. In PPN method every Cluster head (CH) node maintains the neighbor table which is used to keep information about all the nodes. In PPN scheme, in path discovery phase , an intermediate node will attempt to create a route that does not go through a node whose replied information is wrong and PPN is not fully divisible. So that malicious nodes will be avoided by other non-malicious nodes in the network. The proposed scheme applies on those nodes through which source has routed data previously and knows them to be trustworthy) to transfer data packets. All nodes of the network after getting the malicious list finds the Node IDs of the malicious nodes in their table and each node flushes all the entries related to these Node IDs from the respective tables.

3. PROPOSED WORK

It is seen that different types of attack cause the degrade of the network performance , so to overcome this problem we need to develop a method that identify the malicious node in manet so that data can not be drop.

Proposed Mehod for Detection And Removal Of Black Hole In Manet.

1. Source Broadcast the route request(RREQ) to the network with the help of IAOMDV.

2. After that it get reply message

3. After getting reply it check the TTL for each node .

IF

The TTL is greater than 10 then activate the DSR. DSR protocol request for the route (RREQ) it automatically guide the node for next hop.

ISSN: 2278 – 1323

when we reached to next hope the IAOMDV activated and same cycle has been started.

ELSE If

The value of TTL is less than 10 then

4.It request for the route to the hope through which the data is sent.

5.Then Destination node makes a route reply (RREP).

6. After that the source node sent the data.

7. The data is sent at the destination.

3.2 Protocol Used

DSR: The DSR is Dynamic Source Routing protocol . It is an on demand source routing protocol. It is a simple and efficient routing protocol that is designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. It is a reactive routing protocol. It allows the network to be self-organizing and self configuring, without the the use of any existing network administration.

If the source finds a valid route to the destination, it uses this route to send its data packets. If there is no valid route in the its cache, the sender initiates the route discovery procedure. This is initiated by broadcasting a route request messeges. The route request messages contains the address of the destination, the address of the source, and a unique request ID.

ii) Improved Ad-hoc On-demand Multipath Distance Vector Routing (IAOMDV)

It is Improved Ad-hoc On-demand Multipath Distance Vector Routing (IAOMDV) protocol. It is based on the distance vector concept IAOMDV finds path on demand by using a route discovery procedure. It is used for computing multiple loop-free and link disjoint paths. In IAOMDV only nodes that are disjoint considered in all the paths, so that we achieving path disjointness. we use link disjointness in the hope so that to find more alternate routes in the network. With multiple redundant paths available, when an earlier path fails, the protocol switches routes to a different path .Thus a new route discovery is avoided.

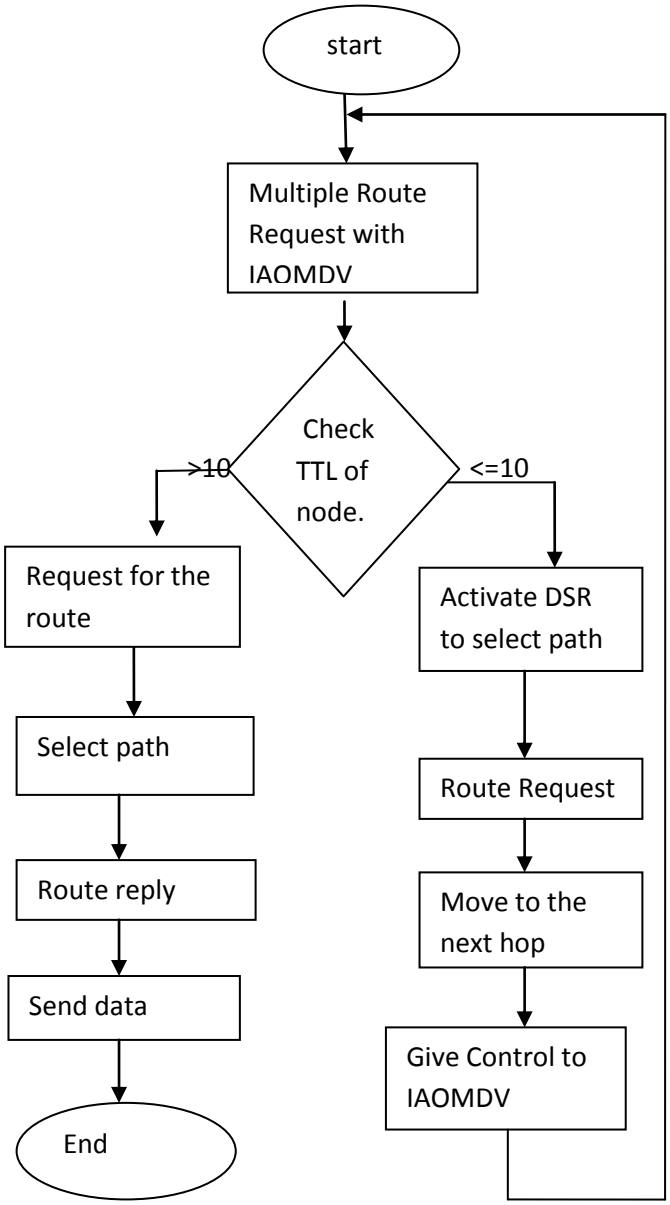

Figure 8: Flow Chart of Proposed System

ISSN: 2278 – 1323

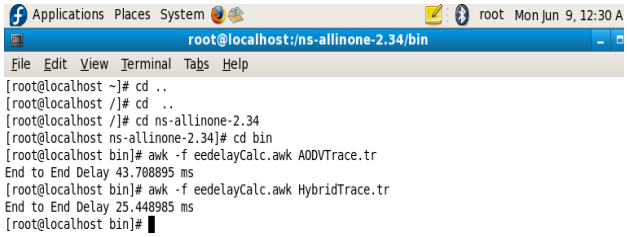

Fig 1 End to end delay

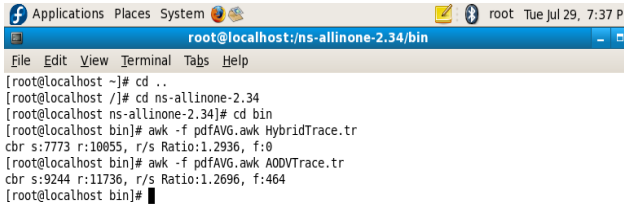

Fig 2 Packet delivery fraction

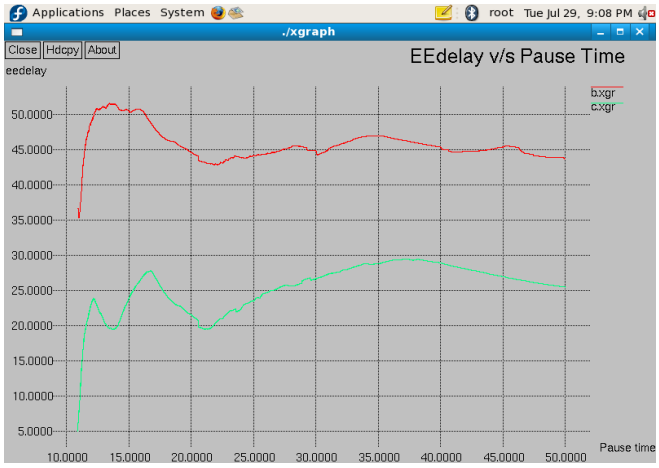

Fig 3 Graph of end to end delay and pause time

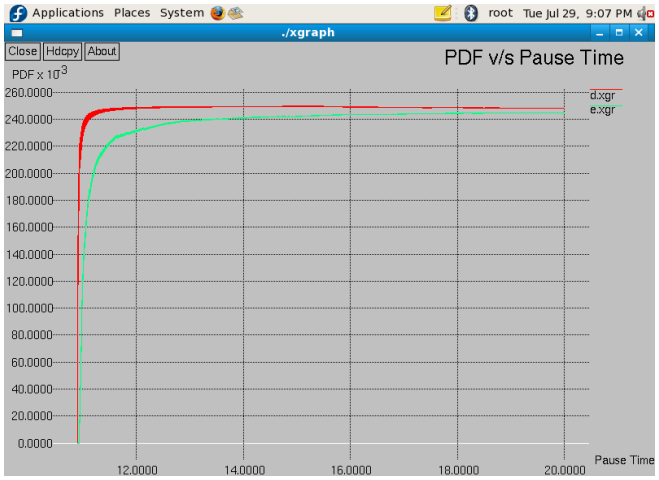

Fig 4 Graph of PDF and pause time

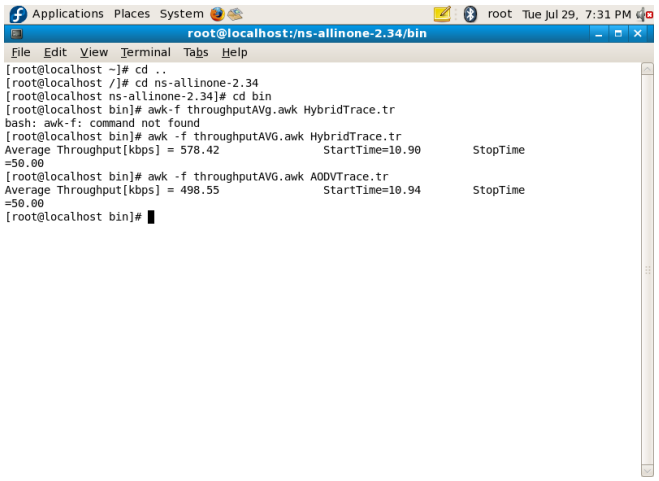

Figure 5 Throughput

ISSN: 2278 – 1323

Table 1 : Simulation Parameter

Parameter	Value
Simulator	NS-2.34
Routing protocol	DSR, IAOMDV
No of nodes	50
Simulation time	50 sec
Propagation Model	Two Ray Ground Reflection model
Simulation area	1000*1000
No of malicious nodes detect	4
Mac Layer	IEEE 802.11

3. CONCLUSION AND FUTURE WORK.

Mobile Ad-Hoc Networks are decentralized wireless systems. MANETs is a collection of mobile nodes that are free in moving in and out in the network. These Nodes are the systems or devices like mobile phone, laptop that are participating in the network and are mobile. Mobile nodes can act as host/router or both at the same time. They can form topologies that are arbitrary ,that depending on their connectivity with each other in the network. These nodes have the ability to ready to use itself and because of their self configure ability, they can be deployed urgently without the need of any challenging and interesting research areas. In the current paper we have presented different aspects of MANETS with different research studies. We have also present the new technique to use two routing protocol as hybrid and checked it is giving better results.In future this method may be implemented with modified version of AODV and DSDV and also with multicast routing protocols such as the On-demand Multicast Routing Protocol (ODMRP). And result for the different performance matrices be scrutinize. In future we can hybrid multicast protocol.

ACKNOWLEDGMENT

Thanks to my Guide and family member who always support, help and guide me during my dissertation.

REFERENCES

[1] Gundeep Singh Bindra, Ashish Kapoor , Ashish Narang , Arjun Agrawal, **"**Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs" international conference on system engenring and technology in 2012.

[2] Sapna Gambhir , Saurabh Sharma "Prime Product Number based Malicious Node Detection Scheme for MANET" in 2012.

[3] Mohammad s. obadiat, Issac wounganag, sunjay kumar "Preventing Packet Dropping and Message Tampering Attacks on AODV-based Mobile Ad Hoc Networks"in 2012.

[4] .Humaira Ehsan Farrukh Aslam Khan "Malicious AODV Implementation and Analysis of Routing Attacks in MANETs" in IEEE conference 2012.

[5] Ashok M.Kanthe, Dina Simunic and Ramjee Prasad " Effects of Malicious Attacks in Mobile Ad–hoc Networks" in IEEEE Conference in 2012

[6] Akshai Aggarwal Gujarat Technological University, and Nirbhay Chaubey "A Simulation Study of Malicious Activities under Various Scenarios in Mobile Ad hoc Networks (MANETs)" in 2012.

ISSN: 2278 – 1323

[7] Prachee N. Patil and Ashish T. Bhole **"**Black hole attack prevention in manet using route ca ching" in IEEE conference 2013.

[8] Sapna Gambhir , Saurabh Sharma "PPN prime Product Number Based Melicious Node Detection Scheme For Manet" in IEEE conference in 2012.

ISSN: 2278 – 1323