TO ENHANCE THE SECURITY AND IMPROVE THE PERFORMANCE OF AODV PROTOCOL IN MANET USING DELAY PER HOP TECHNIQUE

Ankush Mehra
Department of Computer Science GCET
Gurdaspur India

Suraj pal
Department of Computer Science GCET
Gurdaspur India

ABSTRACT
The mobile adhoc network is the decentralized type of network in which mobile nodes can join or leave the network when they want. The ad hoc network is a decentralized type of wireless network. There is no pre-existing infrastructure such as routers in wired networks or access points in wireless networks on which it is depended. The ad-hoc networks are a new standard of wireless communication for mobile hosts. No fixed infrastructure in ad hoc network like base stations is required. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. As MANETs are illustrate by limited bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes, topology changes and unreliable communication in the design. There are many types of protocol are available in MANET. Its efficiency of a routing protocol is determined by its battery power consumption of a participating node and routing of traffic into the network. The security attacks are broadly into active and passive attacks. The wormhole attack is the active type of attack which increase delay in the network. In this research work, technique of delay per hop will be proposed which detect malicious nodes from the network. The proposed algorithm is implemented in Ns2 and results are analyzed in terms of certain parameter. The proposed algorithm performs well in terms of throughput, delay and packet loss.

Index Terms:- Delay, Throughput.

INTRODUCTION
A network is a group of two or more computer systems which linked together. It is mode of exchange of information to communicate with one another. It is a connection of computer devices which are attached with the communication facilities. The physical connection between networked computing devices is established using either cable media or wireless media. Internet is the best-known computer network. When number of computer are joined together to exchange information they form networks and share resources. Networking is used to share information like data communication. Sharing resources can be software type or hardware types. It is central administration system or supports these types of system. World Wide Web application is supported by Computer Network. It shared use of application, use of email and instant messaging applications and storage servers, printers, and fax machines. The communications protocols used to organize network traffic, with the network’s size, its topology and its organizational intent. A network can be wired network and wireless network. Wired network is that which used wires for communicate with each other’s and wireless network is that which communicate without the use of wires through a medium.

1.1 WIRELESS NETWORKS
Wireless Networks term is referring to a kind of networking that do not requires cables to connect with devices during communication. The transmission is take place with the help of radio waves at physical level. Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols and without the using of cables. It is also known as Wi-Fi or WLAN. With the help of this network, devices can be joined easily with the help of radio frequency without wires to sharing information. The IEEE standard for wireless network is 802.11.

1.1.1 INFRASTRUCTURE NETWORKS
In the infrastructure based network, communication is takes place only between the wireless nodes and the access points. The communication is not directly takes place between the wireless nodes. Here the access point is used to control the medium access as well as it acts as the bridge to the wireless and wired networks. In this network, fixed base stations are used when the node goes out of the range of base station another base station come into range. The example of infrastructure based network is cellular networks. It is centralized system which is controlled by the controller like router. The main problem in this system is that if controller fails all the system will crash.

1.1.2 INFRASTRUCTURE LESS NETWORKS
In infrastructure less network does not need any infrastructure to work. In this network each node can communicate directly with other nodes. So in this network no access point is required for controlling medium access. Infrastructure less networks do not have routers that are fixed. In this network all the nodes need to act as routers and all nodes are capable of movement and can be connected dynamically in an arbitrary manner. All the devices in infrastructure less network are wirelessly communicated to each other.
1.2 Ad hoc network

The ad hoc network is a decentralized type of wireless network. There is no pre-existing infrastructure such as routers in wired networks or access points in wireless networks on which it is depended. The ad-hoc networks are a new standard of wireless communication for mobile hosts. Basically it’s a network which is used in urgent situation causes. No fixed infrastructure in ad hoc network like base stations is required. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages.

1.2.1 Types of Ad-hoc Network

There different types of Ad-hoc network available. These are as following:

1. MANET
2. Wireless Sensor Networks (wsn)
3. Wireless Mesh Networks (wmn)

1.2.1.1 MANET

MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. They can act as both routers and hosts. They have ability to self-configure makes this technology suitable for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is urgently required. In MANET routing protocols for both static and dynamic topologies are used.

Mobile Ad hoc Network is a mobile multi-hop which is wireless distributed network and self-organized in nature. The primary objective of routing protocol is to discover the route. In the routing protocol for MANET undertakes to setup and maintain routes between nodes. In MANET, constantly changing network topology causes link breakage and invalidation of end-to-end route. There is highly dynamic nature of wireless network imposes severe restrictions on routing protocols.

1.3.2 Attacks on MANET

There are two types of attacks are present in MANET which break the security of the networks. These attacks are as follow:

1. Passive Attacks
2. Active Attacks

1. Passive Attacks

A passive attack obtains data exchanged in the network without disturbing the communications operation. The passive attacks are difficult to detection. In its, operations are not affected. The operations supposed to be accomplished by a malicious node ignored and attempting to recover valuable data during listens to the channel. Examples of Passive Attacks are snooping and eavesdropping.

2. Active Attacks

An active attack is that attack which any data or information is inserted into the network so that information and operation may harm. It involves modification, fabrication and disruption and affects the operation of the network. Example of active attacks spoofing, impersonation.

Other types of attack are as follow:

1. Internal Attack

In an internal attack from the network the malicious node gains unauthorized access and behave as a genuine node. Internal attacks are as of compromised nodes that are part of the set of connections. Traffic can be analyze between other nodes and may participate in the activities of other networks.

2. External Attack

The external attack is conceded out by the nodes which do not belong to network. It may cause unviability and congestion by sending false information for the network.

3. Wormhole Attack

In wormhole attack, a malicious node, at one location in the network receives packets and to another location in the network tunnels them, to the location where packets are present into the network. When the control messages are routing are tunneled it create disrupted. It is a network layer attack. The two colluding attacker’s tunnel between them is referred as wormhole.

4. Black hole Attack
In this type of attack, the requests are listen by an attacker for the routers in a flooding based protocol. When a request is received by the attacker to the destination node for a route, it creates a reply for the short route and enters into the passageway to do something with the packets passing between them.

5. Denial of Service Attack

The aims of attack are to hit the accessibility of a node and all the nodes in the entire network. The services will not be accessible if the attack is successful. The attacker generally uses battery exhaustion method and radio signal jamming. It has further sub categories:

1. Smurf Attack
2. Distributed denial of services
3. SYN flood attack

6. Byzantine Attack

In this attack, an intermediate compromised node carries out attacks such as creating collision forwarding packets on non-optimal paths, routing loops, and dropping packets selectively which result in interruption or dreadful conditions of the routing services.

7. Jamming

In this attack, attacker wireless medium keeps monitoring initially in sort to verify frequency at which destination node is getting signal from sender. Signal is transmit on that frequency to hindered error free receptor.

8. Man-in-the-middle attack

In this attack, an attacker sits between the sender and receiver and any information being sent between two nodes sniffs by him. In some cases, attacker may masquerade as the sender to communicate with receiver or masquerade as the receiver to reply to the sender. It starts when first attacker sniffs and eve dropped the packets.

9. Replay Attack

In this type of attack an attacker performs a replay attack are repeatedly re-transmitted the valid data to the network injection fort routing traffic that has been previously captured. This attack targets the routes freshness and determines poor security design.

10. Eavesdropping

It is another kind of attack that often happens in the mobile ad hoc networks. Eavesdropping is done to obtain some information that is confidential and keep secret during the communication. The confidential information may consist of the public key, location, private key and id passwords of the nodes. It should be kept away from the unauthorized access because such data are very important to the security state of the nodes.

1. Literature Survey

Prof. Teodora Bakardjieva et al. explained the basic of networking and their types of connections like peer-peer and client-server types of network connection. In this paper he also introduced about the different types of cables used in networking and about the NIC card. Then he discussed about the Hub and switches. After that the wireless LAN and different types of other networks, their components, advantages and disadvantages of wlan. The different types of network topologies used in computer networks are also mentioned in it. After that different types of applications of computer network and different types of devices used in wireless networks and wired network are explained in this paper.

Tim Groth et al. described about the 802.11 are a family of specifications developed by the IEEE for wireless LAN. It is also known as WI FI. A brief introduction to 802.11 is given including physical layer, and link layer. Also various extensions are listed. Security is briefly covered since it takes in even more significance in this wireless environment. It is currently thought that newer generation handsets that work with 3G cell networks will be complimented with 802.11. The potential and realization of putting voice over 802.11 is discussed. Many of the details of 802.11 were described along with some descriptions of some of the new standards about to be ratified. Just as voice over IP in some cases avoids the public switched telephone network, it may be possible for 802.11 phones to avoid the use of cell phone towers thus avoiding a call charge from a cell phone company.

S. Zeadally et al. discussed about the various networking tools accessible for measurements and testing over wide area networks and many of them have constraints, which limit their use to only a select group of users. As a result, the collection of wide area traffic data and their analyses becomes a difficult task, particularly in cases where the test site lacks collaboration support with other sites with which there is desire for traffic measurements to be used in undergraduate/graduate computer networking classes. In this work, they review a selection of some of the tools that can be used for wide area traffic measurements. Our survey highlights the features and characteristics of each tool as well as their limitations.

Asha Ambaikar et al. they discussed many challenges and issues. An ad hoc network is a collection of mobile nodes that dynamically form a temporary network, without the use of existing infrastructure. When two nodes are not within the radio range of one another, they use intermediate nodes to route packets for them. Routing in MANET is a challenging problem which draws researcher's vision, due to nodes mobility, dynamic topology, frequent link breakage, limitation of nodes (memory, battery, bandwidth, and processing power), and lack of central point like base stations or servers. So by
analyzing and comparing different ad hoc routing protocols based on the metric throughput, packet delivery ratio, end to end delay which may give a solution to the challenges in the ad hoc routing in different situations. The mobility of node and intermediate node which may result link failure.

Sunil Kumar and Pankaj Negi et al. discussed about AODV and most of the on demand ad hoc routing protocols use single route reply along reverse path. Fast change of topology causes that the route reply could not come to the source node, i.e. after a source node sends several route request messages; the node obtains a reply message, especially on high speed mobility. This increases both in communication delay and power consumption as well as decrease in packet delivery ratio. To avoid these problems, a “Backward AODV (B-AODV)” which tries multiple route replies. Backward AODV (B-AODV), which has an original aspect compared to other on-demand routing protocols on Ad-hoc Networks: it reduces path fail correction messages and obtains better performance than the AODV and other protocols have proposed. Backward AODV provides good results on packet delivery ratio, power consumption and communication delay. Successful delivery of RREP messages are important in on-demand routing protocols for ad hoc networks.

Ravindra E et al. mentioned about the A mobile Ad Hoc network is a collection of wireless mobile terminals that are able to dynamically form a temporary network without any aid from fixed infrastructure or Centralized administration. In Large scale Ad Hoc networks the terminal mobility may cause radio links to be broken frequently. With reactive protocol such as AODV. This leads to increase in end-to-end delay, packet dropping rate and can reduce the packet delivery rate. In view of such disadvantages, we propose a new Algorithm which introduces a mechanism of link failure prediction and accordingly perform a rapid local route repair. Simulation results shows that a new algorithm reduces end-to-end delay and packet dropping rate and increases packet delivery rate. AODV takes too much time to rebuild the route after a link break along the active route is broken. This time is too long for some application, such as the real time services of voice and video. The route rebuild time can be reduced if to reduce the recommended HELLO interval.

3. Problem Formulation

Inside and outside attacks are possible in MANET, which are responsible for the degradation of the performance of the network. In inside attacks a node within the network become malicious node and it launched attacks on network. In outside attacks a malicious node which is outside the network, it become the member of the networks and then launched the attack on network. In throughput sensitive wormhole attack which drop the packet so that cannot reach to destination and degrade the performance. Here we want to detect the drop detection using ICMP packets which active monitor packets in monitor mode. Monitor node is used in this study, the node other than the monitor node redirects through the other path. So that it can be easily detected. By drop detection performance can be easily improved.

3.1 Scope of the Study

This study has broader scope. When the mobile nodes are mutually true, it leads to the reliable data transmission between the mobile nodes. But the main problem occurs during the drop of the packet. Drop of the packet is due to wormhole attack. Throughput sensitive wormhole attack is due to the drop of the packet. In this malicious node drop the packet so that it cannot be reach destination. By using ICMP packets nodes goes to the monitor mode. Here some other nodes also available than malicious nodes which detect the packet dropping and redirect them to the source node. So here low performance of the system can be improved by prevent them from internal attacks i.e. by detecting packet dropping. Due to packet drop, path is lost easily. In proposed work, monitoring node concept is important in throughput sensitive wormhole attack. This is designed to find out the packet drop nodes. This work will helps to reduce the problem occur in link failure and packet lost problem. Now the performance degradation problem will also improve.

3.2 Objectives

Objectives of the study are as follow:

1. To study and analyze the performance of AODV routing protocol in MANETS
2. To Trigger wormhole attack in AODV protocol and analyze network performance of MANETS
3. To propose novel technique to detect malicious node and isolate it from the network
4. To implement proposed novel technique and analyze results graphically in terms of energy, throughput and delay

4. RESEARCH METHODOLOGY

In this work, technique will be proposed which will detect and isolated malicious nodes from the network. The proposed technique will be based on the monitor mode technique and node rating. In this work, the Network is deployed and in the network source node and destination nodes are defined. The source node will flood route request packets in the network. The adjacent nodes of the destination will respond back to source node with the route reply packets. The source node selects best path from source to destination on the basis of hop count and sequence number. In the proposed technique following steps are used for the node isolation in the network

1. The best path is selected from source to destination on the basis of hop count and sequence number
2. The established path will be tested to isolate malicious nodes from the network. To test the established path the source node send ICMP messages in the network. The nodes receive ICMP messages and go to monitor mode to watch its adjacent nodes
3. The nodes watch its adjacent nodes, the nodes which are malicious gave least rating
4. The nodes in the network which have least rating will be detected as the malicious nodes. The nodes are colored according to their rating values and these colors are red, green and yellow
5. The Delphi technique is applied which gave location of each node and node which have least rating will be isolated from the network using its location in the network

4.1 FLOWCHART

5. Results and Discussion

5.1 Introduction to NS2

Network Simulation is an event based simulator. The network simulator is discrete event packet level simulator. It covers a very large number of different kinds of protocols application of different types of applications and packets. In it scripting language is used. It contains “NAM” files through which animation is run.

Front End- OTCL scripting language is used.
Back End- Programming language is used.

NS2 has different types of agents. In-built protocols are used in it like AODV, DSDV and DSR.

**Fig 1: Deployment of the network**

As shown in figure 1, the wireless adhoc network is deployed in the fixed area and with fixed number of nodes. The network is the decentralized type and nodes can move freely from one location to other location.

**Fig 2: Path establishment**

As shown in figure 12, the wireless adhoc network is deployed in the fixed area and with fixed number of nodes. The network is the decentralized type and nodes can move freely from one location to other location.
As shown in figure 6, the wireless adhoc network is deployed in the fixed area and with fixed number of nodes. The network is the decentralized type and nodes can move freely from one location to other location. The AODV routing protocol is used to establish path from source to destination. The source node flood route request packets in the network for path establishment to destination. The adjacent nodes of destination will reply back to source node with the route reply packets. The best path will be selected between source and destination. The malicious node exits in the path which will trigger wormhole attack and increase delay between source and destination.

Fig 3: Trigger of attack

Fig 4: Isolation of Malicious node
As shown in the figure 11, the source selected best path to destination on the basis of hop count and sequence number. The monitor mode technique is implemented to gave rating to nodes which are in the network. The node which have least rating will be detected as the malicious node in the network.

As shown in figure 1, the energy graph is plotted of the existing and proposed scenario. In the proposed scenario wormhole is isolated from the network which directly leads to reduction in energy consumption of the network. When the energy consumption of network is reduced then the lifetime of the network will be increased due to isolation of malicious nodes in the network.
As shown in the figure 2, the packet loss of the existing scenario in which wormhole attack is triggered and proposed of proposed scenario is shown and it is been analyzed that packet loss is reduced in the proposed scenario due to isolation of wormhole attack in the network.
As shown in figure 3, the throughput graph of proposed and existing scenario is shown and it is been analyzed that throughput can be increased at steady rate due to isolation of wormhole attack in the network. When the packet loss get reduced in the network then throughput will be increased and due to isolation of wormhole attack.

6. Conclusion

The wireless nature of communication makes wireless sensor networks unreliable as any attack with intent to steal the data can do so by deploying malicious nodes in the network. Normally the routing protocols are designed to find shortest path length is determined using hop count as metric. Out of many attacks the wormhole attack is pretty dangerous one as it is launched using two pairs of malicious nodes with create a tunnel by skipping few nodes in between source and destination node. The existing scheme considers the wormhole attacks when there are no intermediate nodes present between destinations. This technique is suitable for scenarios where the path length between source and destination is two hops only. this scheme cannot be used for networks with layer hops between source and destination node. We have proposed a scheme that can detect wormhole in the path having large hop counts. The proposed algorithm can be further compared with the other algorithms which increase security of the network.

7. References


[33] http://www.slideshare.net/sathesh692/homehimanshumane#btnNext

[35] PET, “Issues in Mobile Ad-hoc Networks


Volume: 03, Issue: 01, Pages:1035-1043 (2011)


