A Study on Routing Protocols Technique

Kapil Joshi[1],
[1]CSE Department, UIT,
Uttaranchal University,
Dehradun, India

Neha Chauhan[2]
[2]CSE Department,
IFTM University,
Moradabad, India

Abstract- Routing Protocol, Mobile Ad-Hoc Network's (MANET's) is a collection of multi-hop wireless nodes that communicate with each other without any centralize control or establish infrastructure. The increase in availability and popularity of mobile wireless device has been developed as a wide variety of mobile ad-hoc networking. These days routing is a critical task due to highly dynamic environment. Routing plays a great role in security of entire network. In this paper, we study about Routing Protocols, wireless network, security attacks within a concept of Black hole.

Keyword- MANET, Wireless Network, Routing Protocols, Security, Black Hole

I.INTRODUCTION

After the favourable outcome and popularity of mobile wireless device MANET has given a reason to researchers to develop a vast variety of MANET's protocol to explore the unique transmission opportunities presented by these devices. Transmission done by these devices by using the wireless spectrum in a client server mode. Origin of the word MANET is taken from a Latin word which signifies "for this" or "for this purpose only" [1]. MANET's have merits over traditional network including reduce in infrastructure cost, ease of establishment and fault tolerance.

Wired solution are used for very long time but the demand for wireless solution are increasing rapidly. Wireless technologies such as Bluetooth, IEEE standard 80.11 allow mobile device to establish a mobile ad-hoc network by connecting through wireless medium without any centralized infrastructure [2]. MANET is a swarm of self governing wireless mobile nodes that can interchange data in a non-static manner. Because of the mobile behaviour of nodes the network structure is dynamic. The network is self deploying and decentralize. Ad-Hoc network have some issues which affect the reliability and limit their viability for different environment; lack of centralized structure within MANET where each single node must work as a router and is the reason behind, for task performance of packet routing. This process is done using one or more than one common routing protocol within the MANET [1].

Area where MANET's mainly used are Military scenario, rescue operation, sensor networks, student on campus, conference, etc. Due to highly dynamic nature routing in MANET's is very crucial job. Some demands of MANET's are security, reliability, availability, Quality of Service (QOS), Security of MANET is another major deployment matter. Malicious Nodes can penetrate the network at any moment because of the nature of MANET's that is mobility and wireless So, the security of transferring data in the nodes needs to be deliberate [3].

The Paper is organised as follows, Section 2 discusses the basic needs of a MANET , Section 3 examine an overview on wireless networks in MANET, Section 4 consist of MANET's routing protocols, In section 5 there is a discussion about characteristics, advantages and disadvantages of MANET's and section 6 focuses upon the security and related issues.

II. LITERATURE REVIEW

We have acknowledge several parts of key literature in the environment of MANET routing protocols which highlight early and second generation protocols as well as the security within the field.

Reference [4] signifies that an impactful MANET routing protocol must be equipped to deal with non-static and unpredictable topology changes associated with mobile nodes. This has been explored upon by [2] who propose that in addition to these basic needs; MANET routing protocols should also be decentralize, self-healing and self organising and able to exploit multi-hopping and load balancing, these requirements ensure MANET routing protocols ability to operate autonomously.

III. WIRELESS NETWORK IN MANET

Wireless networking is a way by which telecommunications networks quit that connect between equipment location and the connection in non-favourable geographical conditions through caballing. Wireless technology use a shared communication medium [5].

Wireless network divided into two parts:

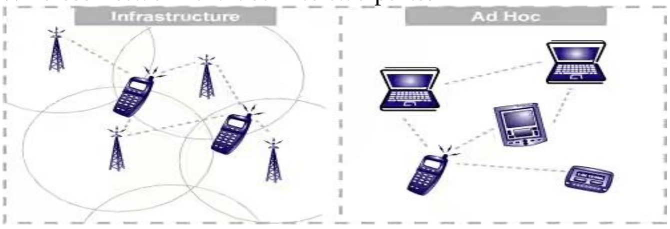


Fig.1 Infrastructure and Infrastructure less Network.

A. Infrastructure Network

Network infrastructure is the hardware and the software resources of an integral networks that enable network connectivity communication, operation and management of an enterprise network. During communication the base station are static and the mobile network are dynamic. If any node crosses the range of one base station, then it will automatically come under the range of another base station.

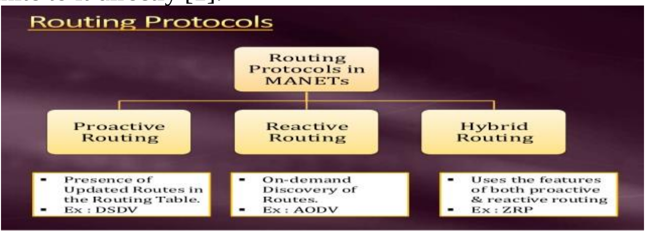
B. Infrastructure less Network

Non-static based station and mobile nodes can move dynamically during communication. Every single node behave as a router. Infrastructure less network called as Ad-Hoc Network. A wireless ad-hoc network is a decentralize type of wireless network which does not based on any infrastructure. It have quit the complexity of infrastructure setup and administration. The ad-hoc network sometimes use flooding for forwarding data

The purpose of routing in MANET is to withhold end to end paths or routes, scaling i.e, minimize overhead and route maintenance.

IV. ROUTING PROTOCOLS

The transmission of information or data packets from source to destination known as Routing. Routing protocol determines how routers impart with each other propagate information that empower them to select routes between any two nodes on a computer network. Routing helps us to specify best route possible whereas router interior knowledge only of networks unite to it directly [1].



Routing Protocols

Routing Protocols in MANETs

Proactive Routing

Reactive Routing

Hybrid Routing

- Presence of Updated Routes in the Routing Table.
- Ex : DSDV

- On-demand Discovery of Routes.
- Ex : AODV

- Uses the features of both proactive & reactive routing
- Ex : ZRP

Fig. 2 Types of Routing Protocol

A. Proactive Routing Protocol

Proactive routing protocol based on maintaining routing tables of known destinations which diminish the amount of control traffic. Packets are progressed immediately using known routes due to which the generation of proactive routing takes place. A well known type of this protocol is Destination Sequenced Distance Vector (DSDV) [6].

1) DSDV: Destination sequenced distance vector is a table driven routing design for ad-hoc mobile networks based on Bellman Ford algorithm to weigh the shortest number of hops to the destination. It was developed by C. Perkins and P. Bhagwat in 1994. Each mobile node exist in the network keep a routing table which contain all feasible destination and number of hops to each destination in the network that are recorded. DSDV uses the mode of sequence number assigned by destination hops to determine the originality of route.

B. Reactive Routing Protocol

Reactive routing protocol build up routes only when required by source node. Minor routing information is the major boon to this protocol. It uses concept of source routing i.e, uses data packet headers embrace routing information meaning nodes do not need routing table; however this has high network overhead, example of this protocol is Ad-hoc on Demand Distance Vector(AODV), Dynamic Source Routing(DSR)[6].

1) AODV: Ad-hoc on demand distance vector deals with node mobility using sequence of early MANET protocol (DSR,DSDV). AODV utilises sequence number and routing beacons from DSDV but perform route discovery using on-demand route request (RREQ). AODV is different to DSR because it uses distance vector routing that require every node in the route to maintain a temporary routing table for the duration of the communication. It uses an expanding ring search mechanism based upon increasing TTL (time to live) to hinder excessive RREQ flooding.

C. Hybrid Routing Protocol

The Hybrid routing protocol is a union of both proactive routing protocol and reactive routing protocol, typically seeking to exploit the reduce control traffic overhead from proactive systems whilst narrow the route discovery delays of reactive systems by maintaining some form of routing table. Hybrid protocol have higher latency than proactive routing protocol, its example are Zone Routing Protocol (ZRP), Zone Based Hierarchical Link State(ZBHL)[6].

1) ZRP: To acquire advantage zone routing protocol uses proactive and reactive protocols for routing between these two adjacent nodes. ZRP divide network into different size overlapping zones. Every zone consist of two types of nodes, i,e. Peripheral nodes and interior nodes, where peripheral nodes are placed at extreme and interior node are at in the radius zone.

V. CHARACTERSTICS OF MANET

- ➢ Autonomous behaviour as each node act as both host and router.
- ➢ Dynamic topology, because the nodes can join or leave the network any time.
- ➢ MANET are capable of Multi-hop routing, when a source node and destination node for a message is out of the radio range.
- ➢ Distributed operation for security, routing and host configuration.
- ➢ Light weight terminal as mobile node are characterized with less money, power.
- ➢ Energy constrained and limited bandwidth.

All node have identical features with similar responsibilities, capabilities and, hence it forms a completely symmetric environment [7]. A MANET environment has some advantages and disadvantages.

A. Advantages of MANET

- o According to the geographical location MANET gives access to the information and flexibility.
- o Minimum cost estimation.
- o At any time and place these networks can be arranged.
- o Powerful due to decentralised management.
- o Enhanced flexibility.
- o With dynamic network topology and multi-hop network MANET has dependent behaviour.
- o Self maintained and organise network, nodes can also act as routers.

B. Disadvantages of MANET

- Packet loss due to factors such as hidden terminals that results in collision, wireless channel issues, interference etc.
- Frequent node partitions.
- Insufficiency of physical security.
- Imminent Resources are limited.
- Malicious attacks are hard to recognize due to dynamic nature.
- Mutual trust unsafe to attack.
- Lack of authorization services.

VI.MANET SECURITY GOALS AND ATTACKS

A. Security Goals

Security is a critical phase of MANET. Security involves a set of consideration that are sufficiently funded. Securing a MANET is a challenging job because in MANET all the network functions such as routing and packet forwarding are implemented by themselves in a self-organizing way. The major points that are needed to accomplish security goals are [8]-

- Confidentiality
- Availability
- Authentication
- Integrity
- Non-repudiation

B. Security Attacks

The most challenging task is securing and designing an efficient routing protocol for wireless ad-hoc network. Due to non-static nature and no infrastructure of MANET claims a new set of networking strategies to be processed in order to provide cogent and secure overhead free end-to-end communication. The decrease in the performance of network is because of insufficiency of predefined centralized administration for route discovery procedure. As compare to wired networks, MANET is more delicate to cyber/digital attacks. There are several types of attack that affect the MANET and its security [8].

1) Internal Attacks: Those attacks which directly lead to the attacks on nodes present in networks links interface between them are known as internal attacks. In this form of attacks, it broadcast wrong type of routing information to other nodes[9]. These attacks are more perplexing task to handle as compare to external attacks, because the internal attacks occurs due more trusted nodes. The malicious node generates wrong information and are difficult to identify.

2) External Attacks: These type of attack try to cause redundancy in the network, denial of services (DoS), and advertising wrong routing information etc [9]. Communication between networks and producing additional overhead to network is hindered by external attacks. There are two types of attacks which come under the category of external attacks.

- Passive Attacks
- Active Attacks

There is a most powerful attack named as “BLACK HOLE” attack which comes in the category of Active attacks i.e the type of External Attack. In the next section, the overview on black hole attack has been defined.

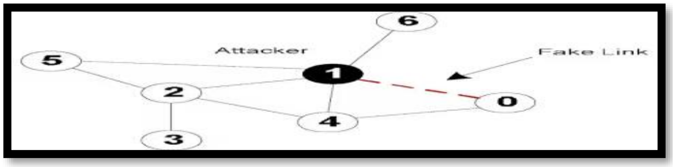
VII. OVERVIEW ON BLACKHOLE ATTACK

In Blackhole attack, the malicious nodes demand on having an optimum route to the node whose packet it want to neutralized. Malicious node sends a fake reply with utmost short route, after receiving the request[10]. Once the node has been able to assign itself between the communicating nodes, it is able to do anything with the packets passing between them.

Blackhole attacks are of two types: Single black hole attack and Cooperatve black hole attack. In single black hole attack, one node advertises itself having the shortest route to the destination and intercepts the packet. In cooperative black hole attack, malicious nodes work in swarms.

A. Detection and Elimination of Black Hole

In order to detect black hole attack, a mechanism based on WATCHDOG has been designed. Watch dog detect misbehaviour nodes by monitoring the transmission of next hop neighbour. In watchdog, the copy of the packets that are forwarded by a node are kept in a buffer and it eavesdrop on the transmission of next link to confirm that it forwards packet properly. The overheard packet is then compared with the packet that is kept in buffer. The packet in the buffer is removed if there is a match, Otherwise, the watch Dog increments the failure count of the node which id responsible for forwarding packets. The node is detected as misbehaving node when the failure count exceeds some threshold value and a notification message is sent to source node.



CONCLUSION

In this paper, we have discussed the overview on MANET (its functionality, features, advantages, disadvantages), Routing protocol, Wireless network and security with the concept of BLACKHOLE, where we have lays emphasis on the keyword that used in the paper, in which we get to know about what is MANET, how important it is and how it has been used and the issues that should kept in mind for the betterment of MANET for a reliable and comfortable result. Too, considered security with their goals and attacks and From all we can conclude that MANET is a swift developing and dynamic field with a vast scope of research work in this field.

REFERENCES

[1] Meenakshi Yadav et.al/Survey on “MANET”, Sunil Taneja and Ashwani Kush, “A Survey of Routing Protocols in Mobile Ad-hoc Network”, International Journal of Innovation, Management and Technology, vol. 1, No. 3, August 2010, ISSN: 2010-0248.

[2] www.ijicse.in,International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.

[3] “For mobile ad-hoc networks”, Ad-Hoc Networks, Vol. 6, No. 8 pp. 1134-1150-2008.

[4] R. O. Schmidt and M. A. S. Trentin, “MANET’s Routing Protocols Evaluation in a Scenario with High Mobility: MANET Routing Protocols Performance and Behaviour”, Network Operations and

Management Symposium, 2008. NOMS 2008. IEEE, Salvador, Bahia, pp. 883-886, 2008.

[5] https://en.m.wikipedia.org/wiki/Wireless_network

[6] Simardeep Kaur,, K .Gupta, RIMT IET, Punjab, India, Dept. Of CSE, RIMT IET, Punjab, India," Position Based Routing in Mobile Ad-Hoc Networks: An Overview," IJCST Vol. 3, Issue 4, Oct- Dec 2012, ISSN: 0976-8491 (online)| ISSN: 2229-4333(print).

[7] http://www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-and-features/

[8] https://www.slideshare.net/mobile/sunitasahu101/attacks-in-manet

[9] Amitabh Mishra," SECURITY AND QUALITIY OF SERVICE IN AD-HOC WIRELESS NETWORKS" (chapter 1,3), ISBN-13 978-0-521-87824-1 Handbook.

[10] Akansha Saini, Harish Kumar, "Effect of Black Hole Attack on AODV Routing Protocol in MANET".