Routing issues and challenges for MANETs: A Review

Ms. Monika kashap*
Student, SVIET, Banur
Mohali

Mr. Sukhvir Singh**
Assistant Professor, UIET
Chandigarh

Ms. Rimpy Kumari***
Assistant Professor, SVIET, Banur
Mohali

Abstract: ***Mobile Ad Hoc Network (MANET) is collection of multi-hop wireless mobile nodes that communicate with each other without centralized administration. A mobile ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. This paper provides an overview of different routing protocols and also provides a comparison between them. Despite many intriguing future applications of mobile ad hoc networks (MANETs), there are still some critical challenges and open problems to be solved. Thus, broadly in this paper we present an overview of MANETs, and their routing protocols. Then we present several challenging issues and the future work.***

1. INTRODUCTION

From last few years wireless networks has become popular. There exist three types of mobile wireless networks: *Infrastructure networks*, *ad-hoc networks* and *hybrid networks* which combine infrastructure and ad-hoc aspects. The term node referred to as a device which is free to move arbitrarily in every direction.

These nodes can be a mobile phone, laptop, personal digital assistance, MP3 player and personal computer which can be located in cars, ships, airplanes or with people having small electronic devices. Research work have been focused on different routing protocols such as Dynamic Source Routing (DSR),

Optimized Link State routing (OLSR), Temporarily Ordered Routing Algorithm (TORA) and Ad hoc On-demand Distance Vector (AODV), for their development and standardization of routing support by MANET working group of Internet Engineering Task Force (IETF). We have observed the effect of these protocols on MANETs.

2. MANET ROUTING PROTOCOLS

There are following types of protocols for MANETs:

Reactive Protocol

Reactive protocols seek to set up routes on-demand. If a node wants to initiate communication with a node to which it has no route, the routing protocol will try to establish such a route.

Proactive Protocol

A proactive approach to MANETs routing seeks to maintain a constantly updated topology understanding. The whole network should, in theory, be known to all nodes. This results in a constant overhead of routing traffic, but no initial delay in communication.

Hybrid Protocol

Hybrid protocols seek to combine the proactive and reactive approaches. There are following main routing protocols for MANETs:

2.1 AODV – (Ad-Hoc On demand Distance Vector)

The philosophy in AODV, like all reactive protocols, is that topology information is only transmitted by nodes on-demand. When a node wishes to transmit traffic to a host to which it has no route, it will generate a *route request* (RREQ) message that will be flooded in a limited way to other nodes. This causes control traffic overhead to be dynamic and it will result in an initial delay when initiating such communication. A route is considered

found when the RREQ message reaches either the destination itself, or an intermediate node with a valid route entry for the destination. For as long as a route exists between two endpoints, AODV remains passive. When the route becomes invalid or lost, AODV will again issue a request.

AODV avoids the "*counting to infinity*" problem from the classical distance vector algorithm by using sequence numbers for every route. The counting to infinity problem is the situation where nodes update each other in a loop. Consider nodes A, B, C and D making up a MANET as illustrated in figure 1.1. A is not updated on the fact that its route to D via C is broken.

This means that A has a registered route, with a metric of 2, to D. C has registered that the link to D is down, so once node B is updated on the link breakage between C and D, it will calculate the shortest path to D to be via A using a metric of C receives information that B can reach D in 3 hops and updates its metric to 4 hops. A then registers an update in hop-count for its route to D via C and updates the metric to 5. And so they continue to increment the metric in a loop.

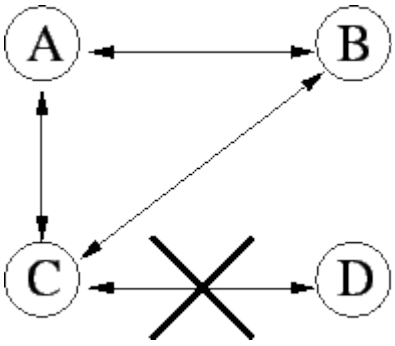

Figure: 1.1 A scenario that can lead to the "counting to infinity" problem.

The way this is avoided in AODV, for the example described, is by B noticing that as route to D is old based on a sequence number. B will then discard the route and C will be the node with the most recent routing information by which B will update its routing table.

AODV defines three types of control messages for route maintenance:

RREQ-A *route request* message is transmitted by a node requiring a route to a node. As an optimization AODV uses an *expanding ring* technique when flooding these messages. Every RREQ carries a *time to live* (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received.

Data packets waiting to be transmitted (i.e. the packets that initiated the RREQ) *should* be buffered locally and transmitted by a FIFO principal when a route is set.

RREP - A *route reply* message is uncased back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can uncast the message back, is that every route forwarding a RREQ caches a route back to the originator.

RERR - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

2.2 OLSR – (Optimized Link State Routing)

It is a table-driven pro-active protocol. As the name suggests, it uses the link-state scheme in an optimized manner to diffuse topology information. In a classic link-state algorithm,

link-state information is flooded throughout the network. OLSR uses this approach as well, but since the protocol runs in wireless multi-hop scenarios the message flooding in OLSR is optimized to preserve bandwidth. The optimization is based on a technique called *Multipoint Relaying*.

Being a table-driven protocol, OLSR operation mainly consists of updating and maintaining information in a variety of tables. The data in these tables is based on received control traffic, and control traffic is generated based on information retrieved from these tables. The route calculation itself is also driven by the tables.

OLSR defines three basic types of control messages

HELLO - *HELLO* messages are transmitted to all neighbors. These messages are used for neighbor sensing and MPR calculation.

TC - *Topology Control* messages are the link state signaling done by OLSR. This messaging is optimized in several ways using MPRs.

MID-*Multiple Interface Declaration* messages are transmitted by nodes running OLSR on more than one interface. These messages list all IP addresses used by a node.

2.3 Hybrids – ZRP (Zone Routing Protocol**)**

An example of such a protocol is the *Zone Routing Protocol* (ZRP). ZRP divides the topology into zones and seek to utilize different routing protocols within and between the zones based on the weaknesses and strengths of these protocols. ZRP is totally modular, meaning that any routing protocol can be used within and between zones. The size of the zones is defined by a parameter *r* describing the radius in hops. ZRP scenario with r set to 1. Intra-zone routing is done by a proactive protocol since these protocols keep an up to date view of the zone topology, which results in no initial delay when communicating with nodes within the zone. Inter-zone routing is done by a reactive protocol. This eliminates the need for nodes to keep a proactive fresh state of the entire network.

ZRP Defines technique called the *Border cast Resolution Protocol* (BRP) to control traffic between zones. If a node has no route to a destination provided by the proactive inter-zone routing, BRP is used to spread the reactive route request.

3. MANET CHALLENGES AND ISSUES

3.1 CHALLENGES

The major challenges faced by the MANETs can be broadly classified as:

a) In incorporating emerging wireless network elements such as MDs, ad-hoc routers and embedded sensors in the existing protocol framework and

b) To provide end-to-end service abstractions that facilitates application development.

These challenges are posed by a broad range of environments such as cellular data services, Wi-Fi hot-spots, Info stations, mobile peer-to-peer, Ad-hoc mesh networks for broadband access, vehicular networks, sensor networks and pervasive systems. These wireless application scenarios lead to a diverse set of service requirements for the future as summarized below:

1. Naming and addressing flexibility.
2. Mobility support for dynamic migration of end-users and network devices.
3. Location services that provide information on geographic position.
4. Self-organization and discovery for distributed control of network topology.
5. Security and privacy considerations for mobile nodes and open wireless channels.

6. Decentralized management for remote monitoring and control.
7. Cross-layer support for optimization of protocol performance.

8. Sensor network features such as aggregation, content routing and in-network processing.

9. Cognitive radio support for networks with physical layer adaptation.

10. Economic incentives to encourage efficient sharing of resources.

3.2 ISSUES

Major issues for MANETs are explained as below:

1. Autonomous- No centralized administration entity is available to manage the operation of the different mobile nodes.

2. *Dynamic topology*- Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network vary timely and are based on the proximity of one node to another node.

3. *Device discovery*- Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection.

4. *Bandwidth optimization*- Wireless links significantly lower capacity than the wired links.

5. *Limited resources* -Mobile nodes rely on battery power, which is a scarce resource. Storage capacity and power are severely limited.

6. *Scalability*- Scalability can be broadly defined as whether the network is able to provide an acceptable level of service even in the presence of a large number of nodes.

7. *Limited physical security*- Mobility implies higher security risks such as peer-to- peer network architecture or a shared wireless medium accessible to both legitimate network users and malicious attackers.

8. *Infrastructure-less and self operated*- Self healing feature demands MANETs should realign itself to blanket any node moving out of its range.

9. *Poor Transmission Quality*- This is an inherent problem of wireless communication caused by several error sources that result in degradation of the received signal.

10. *Ad hoc addressing*- Challenges in standard addressing scheme to be implemented.

11. *Network configuration*- The whole MANET infrastructure is dynamic and is the reason for dynamic connection and disconnection of the variable links.

12. *Topology maintenance*- Updating information of dynamic links among nodes in MANETs is major challenging issue.

4. CONCLUSION AND FUTURE SCOPE

MANETs require a reliable, efficient, and scalable and most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. At present, the general trend in MANETs is toward mesh architecture and large scale. Improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. Propagation, spectral reuse, and energy issues support a shift away from a

single long wireless link to a mesh of short links (as in ad- hoc networks). Large scale ad hoc networks are another challenging issue in the near future which can be already foreseen.

We discuss some typical issues and challenges in the mobile ad hoc networks, most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media and limited battery power. The existence of these vulnerabilities has made it necessary to find some effective security solutions and protect the mobile ad hoc network from all kinds of security risks.

During the survey, we also find some points that can be further explored in the future, such as some aspects of the intrusion detection techniques can get further improved. We will try to explore deeper in this research area.

Ad hoc networks, the most talked about term in wireless technologies, approach to be the emperor of future *airs* provided the vision of "anytime, anywhere" communications. At present, the general trend is toward mesh architecture and large scale. New applications call for both bandwidth and capacity, which implies the need for a higher frequency and better spatial spectral reuse. Propagation, spectral reuse, and energy issues support a shift away from a single long wireless link (as in cellular) to a mesh of short links (as in MANETs). Research on "multi-hop" architecture showed it a promising solution to the implementation of ad hoc networks. As the evolvement goes on, especially the need of dense deployment such as battlefield and sensor networks, the nodes in MANETs will be smaller, cheaper and capable. Overall performance of AOMDV is better than others.

REFERENCES

[1] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," in Proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[2]Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2010.

[3] S.Corson, J. Macker, "Routing Protocol Performance Issues and Evaluation Considerations", Request for Comments – 2501, Network Working Group.

[4] Johnson, D., "The Dynamic Source Routing protocol for Mobile Ad hoc networks(DSR)" , IETF internet draft, Draft-item - manet-dsr-09.txt, April 2003.

[5] Johnson,D.B., Maltz,D.A., and Broch,J., "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Ad Hoc Networking, pp.139-172,2001.

[6] IIyas, M., 2003. The hand book of ad -hoc wireless networks. CRC press LLC.

[7] A Mishra and K.M Nadkarni, security in wireless Ad -hoc network, in Book. The Hand book of Ad Hoc Wireless Networks (chapter 30), CRC press LLC, 2003.

[8] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," in Proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[9] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2010.

[10] Janne Lundberg, Routing Security in Ad Hoc Networks. Tik-1,./10.501 Seminar on Network Security.