MANET A REVOLUTION IN NETWORKS

G.S.RAGHAVENDRA, M.V.P UMA MAHESWARA RAO
Assistant Professor, CSE
Andhra Loyola Institute of Engineering and Technology
Vijayawada, Andhra Pradesh
raghavendragunturi@rocketmail.com

Abstract— **Over recent years, the market for wireless communications has enjoyed an unprecedented growth. Wireless technology is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day using pagers, cellular telephones, laptops, various types of personal digital assistants (PDAs) and other wireless communication products. With tremendous success of wireless voice and messaging services, it is hardly surprising that wireless communication is beginning to be applied to the realm of personal and business computing. No longer bound by the harnesses of wired networks, people will be able to access and share information on a global scale nearly anywhere thinks about a Mobile Ad hoc Network (MANET is one that comes together as needed, not necessarily with any support from the existing infrastructure or any other kind of fixed stations. We can formalize this statement by defining an ad hoc (ad-hoc or adhoc) network as an autonomous system of mobile hosts (MHs) (also serving as routers) connected by wireless links, the union of which forms a communication network modeled in the form of an arbitrary communication graph.**

Index Terms: Adhoc, wireless, MANET, interoperation, security, routing

I. INTRODUCTION

In a MANET, no infrastructure exists and the network topology may dynamically change in an unpredictable manner since nodes are free to move.

As for the mode of operation, ad hoc networks are basically peer-to-peer multi-hop mobile wireless networks where information packets are transmitted in a store-and-forward manner from a source to an arbitrary destination, via intermediate nodes as shown in Figure 1.1. As the MHs move, the resulting change in network topology must be made known to the other nodes so that outdated topology information can be updated or removed. For example, as the MH2 in Figure 1.1 changes its point of attachment from MH3 to MH4 other nodes part of the network should use this new route to forward packets to MH2. We assume that it is not possible to have all MHs within range of each other. In case all MHs are close-by within radio range, there are no routing issues to be addressed.

In Figure 1.1 MH1 is within radio range of MH3, then MH3 is also within radio range of MH1. This is to say that the communication links are symmetric. The issue of Symmetric and asymmetric links is one among the several challenges encountered in a MANET. Another important issue is that different nodes often have different mobility patterns. Some MHs are highly mobile, while others are primarily stationary. It is difficult to predict a MH's movement and pattern of movement.

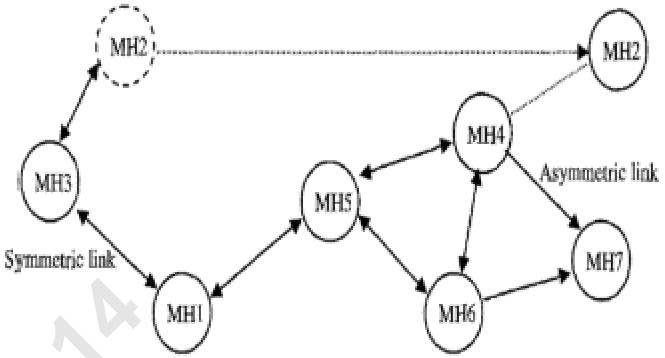

Figure 1.1 - A mobile ad hoc network

II. CHARACTERISTICS

A .Dynamic Topologies

Nodes are free to move arbitrarily with different speeds, thus the network topology may change randomly and at unpredictable times.

B. Energy-constrained Operation

Some or all of the nodes in an ad hoc network may rely on batteries or other exhaustible means for their energy. For these Nodes, the most important system design optimization criteria May be energy conservation.

C. Limited Bandwidth

Wireless links continue to have significantly lower capacity than infrastructure networks. In addition, the realize throughput of wireless communications - after accounting for the effects of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

D. Security Threats

Mobile wireless networks are generally more prone to physical security threats than fixed-cable nets. The increased possibility

of eavesdropping, spoofing, and minimization of denial-of service type attacks should be carefully considered.

III. Routing in Ad Hoc Networks

A. Topology-Based routing

Topology-based routing protocols depend on the information about existing links in the network and utilize them to carry out the task of packet forwarding. They can be further Sub divided as being Proactive (or table-driven), Reactive (or on demand), or Hybrid protocols. Proactive algorithms employ classical routing strategies such as distance-vector or link-state routing and any changes in the link connections are updated periodically throughout the network. Reactive protocols employ a lazy approach whereby nodes only discover routes to destinations on-demand. Hybrid protocols combine local proactive and global reactive routing in order to achieve a higher level of efficiency and scalability.

a. Destination-Sequenced Distance-Vector Protocol:

The destination-sequenced distance-vector (DSDV)[1] is a proactive hop-by-hop distance vector routing protocol, requiring each node to broadcast routing updates periodically. Here, every MH in the network maintains a routing table for all possible destinations within the network and the number of hops to each destination. Each entry is marked with a sequence number assigned by the destination MH. The sequence numbers enable the MHs to distinguish stale routes from new ones, thereby avoiding the formation of routing loops. Routing table updates are periodically transmitted throughout the network in order to maintain consistency in the tables. To alleviate potentially large network update traffic, two possible types of packets can be employed: full dumps or small increment packets. A full dump type of packet carries all available routing information and can require multiple network protocol data units (NPDUs). These packets are transmitted less frequently during periods of occasional movements. Smaller incremental packets are used to relay only the information that has changed since the last full dump. Each of these broadcasts should fit into a standard-size NPDU, thereby decreasing the amount of traffic generated.

b. The Optimized Link State Routing Protocol:

The Optimized Link State Routing (OLSR) protocol is a proactive protocol based on the link state algorithm. In a pure link state protocol, all the links with neighboring nodes are declared and are flooded in the entire network. OLSR [2] protocol is an optimization of a pure link state protocol for MANETs. First, it reduces the size of control packets: instead of all links, it declares only a subset of links amongst its neighbors which serves as its multipoint relay selectors (described next). Secondly, it minimizes flooding of this control traffic by using only the selected nodes, called multipoint relays, in diffusing its messages throughout the network. Apart from normal periodic control messages, the protocol does not generate extra control traffic in response to link failures or additions. The protocol keeps the routes for all the destinations in the network, hence it is beneficial for the traffic patterns with a large subset of MHs are communicating with each other, and the <source, destination> pairs are also changing with time. The protocol is particularly suitable for large and dense networks, as the optimization done using the multipoint relays.

B.POSITION-Based routing

Position-based routing algorithms overcome some of the limitations of topology-based routing by relying on the availability of additional knowledge. These position-based protocols require that the physical location information of the nodes be known. Typically, each or some of the MHs determine their own position through the use of the Global Positioning System [3] (GPS) or some other type of positioning technique.

Two main packet forwarding schemes can be defined for position based routing:

a. Greedy forwarding
b. Restricted directional flooding;

a. Greedy Packet Forwarding:

Using greedy packet forwarding, the sender of a packet includes an approximate position of the recipient in the packet. This information is gathered by an appropriate location service When an intermediate node receives a packet, it forwards the packet to a neighbor lying in the general direction of the recipient. Ideally, this process can be repeated until recipient has been reached. Typically, there are three different strategies a node can use to decide to which neighbor a given packet should be forwarded [4].

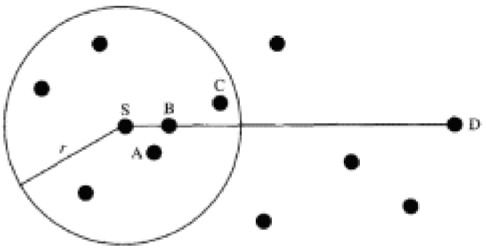

Fig 2.Greedy packet forwarding strategies

where node S and D denote the source and destination nodes of a packet, respectively. The circle with radius *r* indicates the maximum transmission range of node S. One intuitive strategy is to forward the packet to the node that makes the most progress towards node D. In Figure 2 this would be node C. This strategy is known as *most forward within r* (MFR). MFR tries to minimize the number of hops a packet has to transverse in order to reach node D.

Another strategy for forwarding packets is compass routing, in which the neighbor closer to the straight line between sender and destination is selected. In our example of

Figure 2, this would be node B. Compass routing tries to minimize the spatial distance a packet travels. Finally, it is possible to let the sender randomly select one of the nodes closer to the destination than itself and forward the packet to that node. This strategy minimizes the accuracy of information needed about the position of the neighbors and reduces the number of operations required to forward a packet.

Unfortunately, greedy routing may fail to find a path between a sender and a destination, even though one does exist. This can be seen through Figure 3, where the circle around node D has the radius of the distance between nodes S and D, and circle around node S shows its transmission range. Note that there exists a valid path from node S to node D. The problem here is that node S is closer to the destination node D than any of the nodes in its transmission range. Greedy routing has therefore reached a local maximum from which it cannot recover.

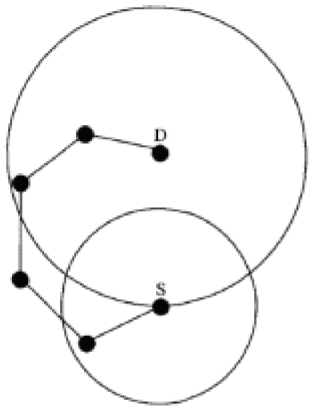

Figure 3 Greedy routing failure

1) *Restricted Directional Flooding*

DREAM:

In DREAM (discussed earlier), the sender node S of a packet with destination node D forwards the packet to all one-hop neighbors that lie "in the direction of node D". In order to determine this direction, a node calculates the region that is likely to contain node D, called the *expected region*. As depicted in Figure 4, the expected region is a circle around the position of node D as it is known by node S. Since this position information may be outdated, the radius *r* of the expected region is set to *(tj - tS)vmax*, where *tj* is the current time, *t0* is the timestamp of the position information node S has about node D, and *vmax* is the maximum speed that a node may travel in the MANET. Given the expected region, the "direction towards node D" for the example in Figure 4 is defined by the line between nodes S and D and the angle (). The neighboring nodes repeat this procedure using their information on node D's position. If a node does not have a one-hop neighbor in the required direction, a recovery procedure has to be started.

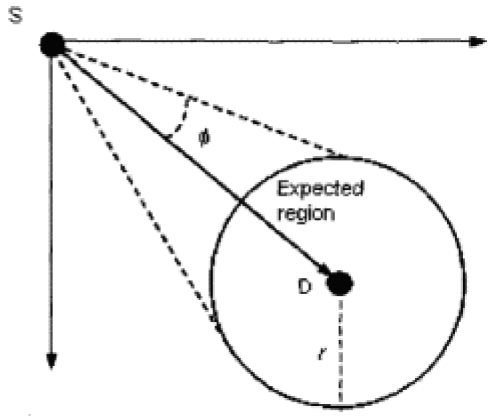

Fig 4 Example of the expected region in DREAM

2) *Location-Aided Routing:*

The Location-Aided Routing[5] (LAR)protocol does not define a location-based routing protocol, but instead proposes the use of position information to enhance the route discovery phase of reactive ad hoc routing approaches, which often use flooding as a means of route discovery. Under the assumption that nodes have information about other node's positions, LAR uses this position information to restrict the flooding to a certain area. This is carried out similar to DREAM.

LAR exploits location information to limit the scope of route request flood employed in protocols such as AODV and DSR. Such location information can be obtained, for example, through GPS. LAR limits the search for a route to the so-called request zone, determined based on the expected location of the destination node at the time of route discovery. Two concepts are important to understand how LAR works: Expected Zone and Request Zone. Let us first discuss what an Expected Zone is. Consider a node S that needs to find a route to node D. Assume that node S knows that node D was at location L at time *t0*. Then, the *"expected zone"* of node D, from the viewpoint of node S at current time *tj*, is the region expected to contain node D. For instance, if node S knows that node D travels with average speed v, then S may assume that the expected zone is the circular region of radius v(ti - t0), centered at location L (see Figure 5(a)).

If actual speed happens to be larger than the average, then the destination may actually be outside the expected zone at time *tj*. Thus, expected zone is only an estimate made by node S to determine a region that potentially all contains D at time *tj*.

Fig 5 Examples of *expected zone*

If node S does not know any previous location of node D, then node S cannot reasonably determine the expected zone (the entire region that may potentially be occupied by the ad hoc network is assumed to be the expected zone). In this case, LAR reduces to the basic flooding algorithm. In general, having more information regarding mobility of a destination node can result in a smaller expected zone as illustrated by Fig 5(b). Based on the expected zone, we can define the request zone. The proposed LAR algorithms use flooding with one modification. Node S defines (implicitly or explicitly) a *request zone* for the route request. A node forwards a route request *only if* it belongs to the request zone (unlike the flooding algorithm in AODV and DSR).

To increase the probability that the route request will reach node D, the request zone should include the *expected zone[6]* (described above). Additionally, the request zone may also include other regions around the request zone. Based on this information, the source node S can thus determine the four corners of the expected zone. For instance, in Fig 6 if node I receives the route request from another node, node I forwards the request to its neighbors, because I determines that it is within the rectangular request zone. However, when node J receives the route request, node J discards the request, as node J is not within the request zone this algorithm is called LAR scheme 1.

The LAR scheme 2 is a slight modification to include two pieces of information within the route request packet: assume that node S knows the location (Xd; Yd) of node D at some time to - the time at which route discovery is initiated by node S is ti, where ti > t0. Node S calculates its distance from location (Xd; Yd), denoted as DISTS [7], and includes this distance with the route request message.

The coordinates (Xd; Yd) are also included in the route request packet. With this information, a given node J forwards a route request forwarded by I (originated by node S), if J is within an expected distance from (Xd; Yd) than node I.

IV. CONCLUSION

With tremendous success of wireless voice and messaging services, it is hardly surprising that wireless communication is beginning to be applied to the realm of personal and business computing. No longer bound by the harnesses of wired networks, people will be able to access and share information on a global scale nearly anywhere thinks about a Mobile Ad hoc NETwork (MANET is one that comes together as needed, not necessarily with any support from the existing infrastructure or any other kind of fixed stations. We can formalize this statement by defining an ad hoc (ad-hoc or adhoc) network as an autonomous system of mobile hosts (MHs) (also serving as routers) connected by wireless links, the union of which forms a communication network modeled in the form of an arbitrary communication graph.

V. REFERENCES

[1] E. Ayanoglu, C.-L. I, R. D. Gitlin, and J. E. Mazo. Diversity coding for transparent self-healing an fault-tolerant communication networks. IEEE Transactions on Communication, 41(11):1677–1686, November 1993.

[2] M. Castro and B. Liskov. Practical Byzantine fault tolerance. In Proceedings of the 3rd USENIX Symposium on Operating System Design and Implementation (OSDI'99) , pages 173–186, New Orleans, LA USA, February 22–25, 1999. USENIX Association, IEEE TCOS, and ACM SIGOPS.

[3] Y. Desmedt. Threshold cryptography. European Transactions on Telecommunications, 5(4):449–457, July–August 1994.

[4] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In G. Brassard, editor, Advances in Cryptology— Crypto'89, the 9th Annual International Cryptology Conference, Santa Barbara, CA USA, August 20–24, 1989, Proceedings, volume 435 of Lecture Notes in Computer Science, pages 307–315. Springer, 1990.

[5] Y. Desmedt and S. Jajodia. Redistributing secret shares to new access structures and its applications. Technical Report ISSE TR-97-01, George Mason University, July 1997.

[6] A. Ephremides, J. E. Wieselthier, and D. J. Baker. A design concept for reliable mobile radio networks with frequency hopping signaling. Proceedings of the IEEE, 75(1):56–73, January 1987.

[7] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In Proceedings of the 28th Annual Symposium on the Foundations of Computer Science, pages 427–437. IEEE, October 12–14, 1987.