Experiment # 5:

Overview on Ad hoc Routing Protocols and Case Study on DSR

Ad hoc networks do not rely on a pre-established infrastructure; therefore, they can be deployed in places with no fixed infrastructure. Wireless mobile ad hoc networks (MANETs) are best suited for conference meetings, lectures, crowd control, search and rescue, disaster recovery, on-the-fly conferencing applications, networking intelligent devices, and automated battlefields. Typically such applications do not have infrastructure or central administration available.

Because nodes are forwarding packets to each other, some sort of routing protocol is necessary to make routing decisions. Currently, there is no existing standard for routing protocols for ad hoc networks. Each host has a wireless interface and communicates directly via radio packets or infrared connections. One feature of ad hoc networks is that the network does not collapse just because one of the mobile nodes moves out of the transmitting range of the other nodes. Nodes should be able to enter/leave the network as required. For instance, if a node leaves the network and caused link breakages, the affected nodes can easily request/find new routes. In other words, ad hoc networks are capable of handling topology changes and malfunctions in nodes. In ad hoc networks, each host must act as a router, since routes are mostly multi-hop, due to the limited power transmission set by government agencies, (e.g. the Federal Communication Commission (FCC), which is 1 Watt in Industrial Scientific and Medical (ISM) band). Due to the continuous movement of the nodes, the backbone of the network is continuously reconstructed. Moreover, the nonexistence of a centralized authority complicates the

problem of medium access. QoS communications in wireless mobile ad hoc network is highly dependent on routing protocols and medium access control (MAC) protocols.

The routing protocols can be classified into three classes according to the way routes are created and maintained:

a) Table Driven Routing Protocols.

b) On-demand Routing Protocols.

c) Cluster-based Routing Protocols.

In wireless networks it is very important to reduce transmission overhead and power consumption due to the limitation of the wireless channel. MANETs have several salient characteristics that have to be taken into account when considering their design and deployment:

- **Dynamic topologies:** Nodes are free to move arbitrarily; thus, the network topology, which is typically multi-hop, may change randomly and rapidly at unpredictable times. This means that we need a mobile infrastructure that quickly adapts to topology changes.
- **Bandwidth-constrained, variable capacity links:** Wireless links typically have significantly lower capacity than their hardwired counterparts. Also, the realized throughput of wireless communications (after accounting for the effects of multiple access, fading, noise, and interference conditions) is often much less than a radio's maximum transmission rate.
- **Energy-constrained operation:** Some or all the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, a finite energy capacity may be the most significant performance constraint, and thus, its

utilization should be viewed as a primary network control parameter.

- **Limited physical security:** Mobile wireless networks are generally vulnerable to impersonation attacks. The increased possibility of eavesdropping, spoofing and denial-of-service attacks should be carefully considered. Authentication and encryption is probably the way to go and the problem lies with distributing keys among the nodes in ad hoc networks.
- **Multiple routes:** To reduce the number of reactions to topological changes and congestion, multiple routes could be used. If one route has become invalid, it is possible that another stored route could still be valid and thus enhance the robustness of the routing protocol.
- **Load balancing:** The protocol should distribute and balance the load amongst all the nodes in the network. It should not be dependent on certain nodes to do the routing. All the nodes should participate in the routing function. This enlarges the life of the network and reduces the reduction of connectivity problem.
- **Loop free:** To improve the performance of the routing protocol, it should guarantee that the routes supplied are loop-free. This avoids any waste of bandwidth or any power consumption.

1. Dynamic Source Routing

Dynamic Source Routing (DSR) is designed to allow nodes to dynamically discover a source route across multiple network hops to any destination in the ad hoc network. When using source routing, each packet to be routed carries in its header the complete, ordered list of nodes through which the packet must pass. A key advantage of source

routing is that intermediate hops do not need to maintain routing information in order to route the packets they receive, since the packets themselves already contain all necessary routing information. Source routing has been used in a number of contexts for routing in wired networks, using their actually defined or dynamically constructed source routes. DSR allows nodes to dynamically discover a route in a multi-hop network to any destination. In DSR, mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. When new routes are learned, entries in the route cache are continually updated. When a mobile station needs to establish a connection to another mobile station, it dynamically determines one based on cached information and on the results of a route discovery protocol. An MT initiating route discovery broadcasts a Route Request (RREQ) packet to its one-hop neighbours. The RREQ contains the address of the destination. Every RREQ packet is uniquely identified by the pair <source address, broadcast id>. To limit the number of RREQs propagated on the outgoing links of a mobile node, it does not forward the RREQ if it was seen by the mobile station. Therefore, when a mobile node receives a RREQ packet it checks the <source address, broadcast id> pair. It appends its own address to the list of addresses in the route record of the RREQ and forwards the packet to its neighbors, only if it had not previously received a RREQ with an identical <source address, broadcast id> pair, and it is not the destination. For example, in Figure 1, MT 2 appends its own address to the RREQ it receives from 1. MT 5, on the other hand, receives two copies of the RREQ. It appends its address to the first copy, i.e., the copy it receives from MT 2. MT 5 discards the RREQ it receives from MT 4, since it previously received a RREQ with the same <source address, broadcast id> pair.

If the receiver of the RREQ is the destination itself, then it sends a route reply (RREP) packet to the source after including a copy of the reversed route record of the received RREQ, in the RREP packet.

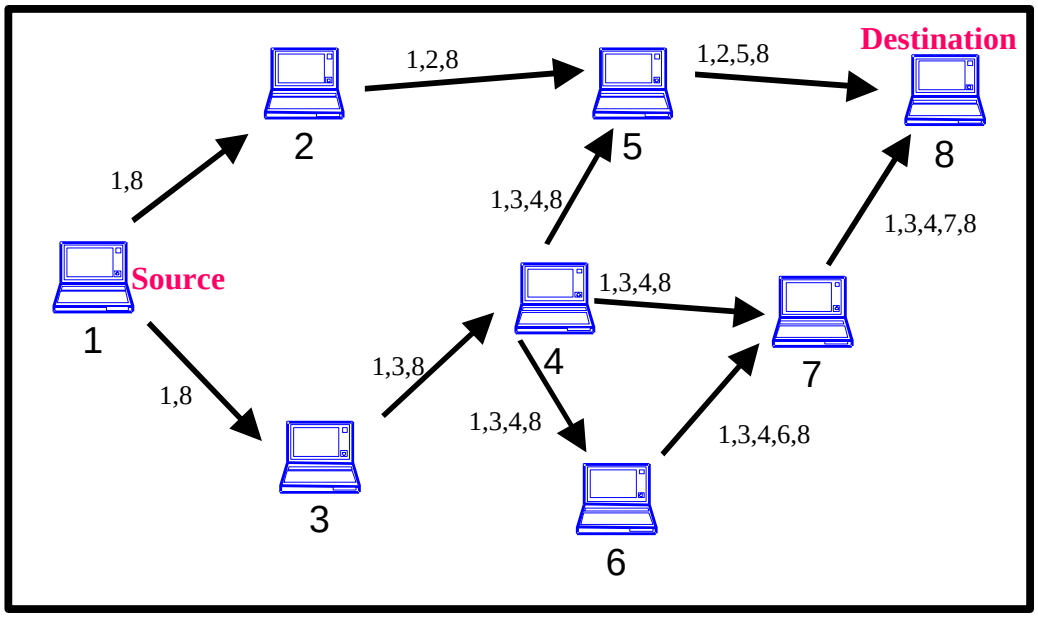

Figure1: Building of the Route Record during Route Discovery in DSR

Figure 2 demonstrates a scenario where a destination, i.e., MT 8, replies with a RREP packet upon the receipt of a RREQ from MT 1. MT 8 receives MT 5's copy of the RREQ before the copy broadcasted by MT 7.

As a result, it appends its own address to the route record of the RREQ received from MT 5, and includes a copy of the reversed route record in the RREP packet. Afterwards, MT 8 forwards the RREP packet to MT 5.

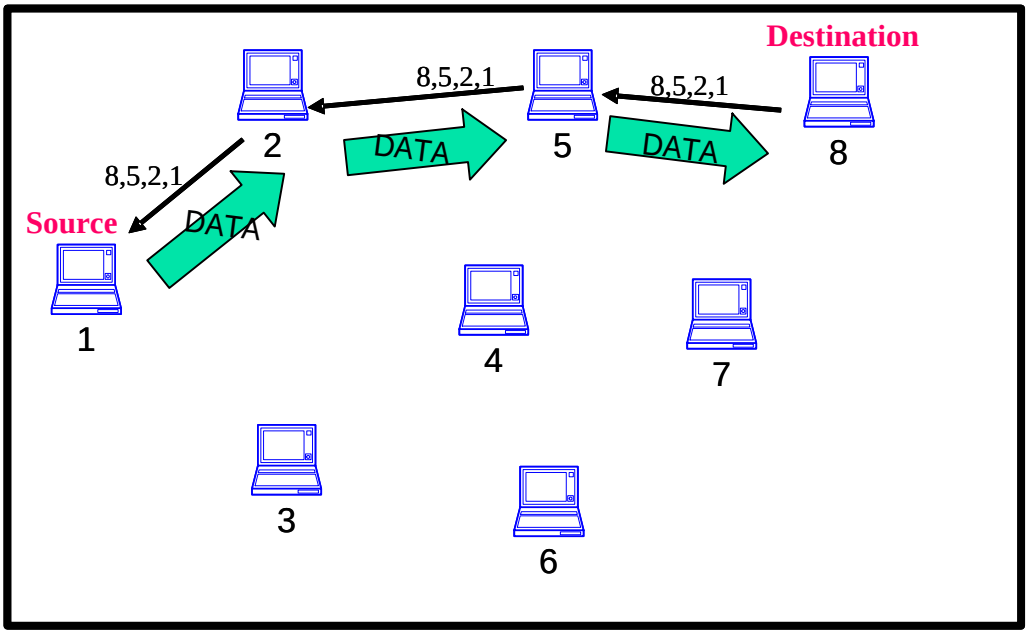

Figure 2: Propagation of the Route Reply with the Route Record in DSR

2. Route Maintenance

DSR provides a method for route maintenance. This is important because the dynamic nature of mobile networks can affect existing routes, and hence, disrupt ongoing communications. For example, it might happen that a mobile station listed in a source route moves out of wireless transmission range, or is turned off, resulting in the corresponding route being unusable. The route maintenance procedure monitors the operation of routes and notifies the sources of any route errors. Route maintenance in DSR can be carried out in two different ways depending on whether the data link layer supports acknowledgements or not. The first method utilizes the hop-by-hop acknowledgements at the data link level to detect lost or corrupted packets, and hence, perform retransmissions. The MT transmitting the packet will be able to determine whether the hop to which it transmitted the packet is still functioning or not. A route error

(RERR) packet is sent to the original sender whenever the data link layer reports a problem from which it cannot recover. The method of passive acknowledgement is utilized in networks that do not support such lower-level acknowledgements. This method relies on the fact that the sender of a packet may be able to hear the receiver's transmission of the packet to the next hop along the path to the destination. The source, upon the receipt of the RERR packet restarts the route discovery process. This is also a major drawback of DSR since route discovery must be restarted form the source.

3. Disadvantages of DSR

DSR is not scalable to large networks, because of the source routing requirement. Furthermore, the need to place the entire route in both route replies and data packets causes a significant overhead.