Routing Protocols for Wireless Ad Hoc Wireless Networks: A Review of the On-Demand Routing Protocols.

Amr Ergawy
aergawy@cc.hut.fi

Abstract

Wireless Ad hoc networks have thier own very specific features. They have dynamically changing topologies, along with relatively limited resources of the transmission medium and the mobile nodes. On demand routing protocols were introduced to adapt with these features of the ad hoc network. This paper reviews this class of protocols.

1 - Introduction

The highly dynamic nature of the wireless ad hoc networks imposes it own requirements on proposed routing protocols for this type of networks. At the same time, on-demand routing protocols are designed to dynamically adapt with the changes of topology and link states of a network. Consequently, on-demand routing protocols are considered as a very important candidates to accomplish the routing function for ad hoc wireless networks.

However, on-demand routing protocols depend mainly on a reactive route establishment process. In the very basic form of this process, a route request packet is flooded across the network. In response, a route reply packet is sent from the addressed destination. This process introduces routing overhead and route establishment delays. Similar problem are also introduced by the similar route maintenance mechanism of these protocols. Consequently, different optimization techniques are introduced by the different on demand routing protocols to reduce such overheads and delays.

This papers review a group of the already proposed on-demand routing protocols. It focuses on the key features of each protocol. Particularly how a protocol establishes routes, and how it reconfigures routes after a link break. Additionally, the advantages and disadvantages of the different protocols are discussed with any possible comparison with the peer protocols.

2 – Dynamic Source Routing Protocol (DSR):

The key feature of this protocol is that it is a pure on demand protocol. Particularly, DSR does not employ any periodic exchange of packets. It does even use beacon packets like some other on demand protocols.

Consequently, DSR applies on demand schemes for both route discovery and route maintenance. This makes the routing overhead traffic scales to the actual needed size automatically. This is considered as the main advantage of DSR. [2]

On the other hand, DSR employs source routing. This means that, each data packet contains the full path which it should traverse to its destination. Source routing is some times considered as a disadvantage of DSR. [1]

For route discovery [1, 2], a node ,which wants to send packets to a specific destination, floods the network with a route request packet. This packet is flooded by all intermediate nodes in the network. The route request packet is initiated with a sequence number which is used by the intermediate nodes to avoid the loop forwarding.

Before an intermediate node propagates the received route request packet, it adds its own address to this packet. Consequently, when this packet arrives to the destination node, it will contain the traversed path to this destination. Figure 1. Shows this route discovery process. The traversed paths are included in the route request packets.

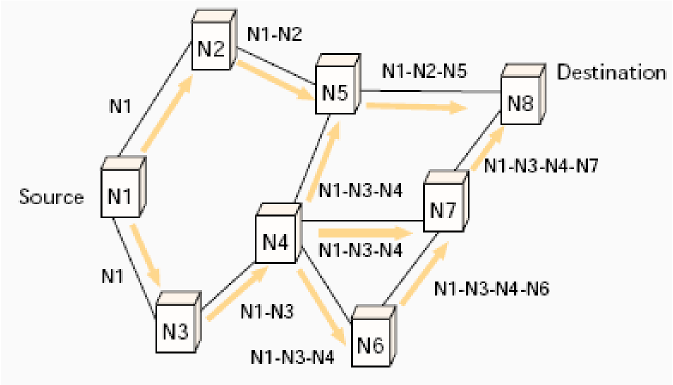

Figure 1. The route discovery process in DSR. [2]

In turn, when the destination node receives the route request packet, it replies by a route reply packet to the source node. This packet is sent along the same path which the route request packet has already traversed before. Particularly, this is considered as the selected route.

Figure 2. Shows the route reply process across the selected route.

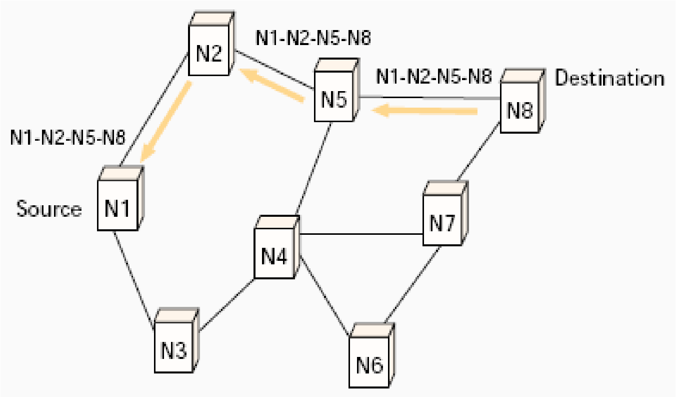

Figure 2. The route reply process in DSR. [2]

The routing discovery mechanism is optimized by using route caching at the intermediate nodes. To maintain its own cache, each node gathers all possible information from the forwarded data packets on the network. This is possible because DSR depends on source routing. This means that the forwarded data packets contain valid routes to their destinations. At the same time, nodes can even listen to the traffic which is not directed to them, by working in the promiscuous mode [1].

Consequently, the cache of a node may contain information about valid routes to specific destinations in the network. As a result, if an intermediate node has a route to a required destination, it will respond to a route request packet which requires this destination. In turn, if a source node receives more than one route reply packet, it will choose the best route depending on an applied metric.

The route maintenance mechanism is applied only when a link break occurs during a session [2]. Simply the closest node to the source ,which detects the break, notifies the source node about the break. The source node ,in turn, invokes the route discovery procedure again to find an alternative route.

3 – <u>Ad Hoc On-Demand Distance-Vector Routing Protocol (AODV)</u>:

The key feature of this protocol is applying a distributed routing scheme. In contrast to the source routing applied by DSR, AODV depends on storing the next hops of a path as entries in the intermediate nodes. From the view point of the size of the packet and bandwidth consumption, this is considered as an advantage of AODV. However, this may require additional resources ,from the intermediate nodes, to maintain the next hop entries. This is considered as a main negative side of AODV. [1].

The route discovery mechanism of AODV can be described as follows. When a source node has packets to send to a destination node, it initiates a route request packet. This packet contains the source address, a sequence number for the source, a sequence number for the destination, a broadcast ID and a hop count. Each piece of information in this packet has is used for a specific purpose in the route setup process. [3]

When an intermediate node receives a route request packet, it checks the broadcast ID and the source address, if it has received the same request before it will drop the packet. Other wise, the node checks whether it has a route to the required destination.

If an intermediate node does not have a route to the addressed destination, it will build what is called a reverse path entry. Then it will forward the packet to its neighbors. In the reverse path entry, an intermediate node keeps track of which node it has received the route request from. In turn when the this node receives a route reply packet, it will forward this packet back towards the source via this reverse path. The reverse path entry will be deleted after some defined time if no route reply packet is received by the intermediate node.

Figure 3. Shows the process of establishing the reverse paths during the route discovery process in AODV.

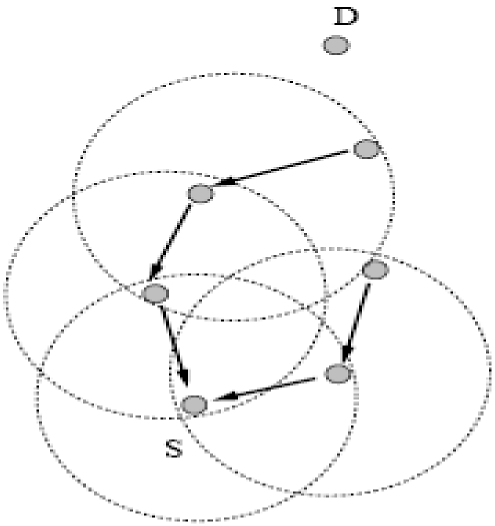

Figure 3. The reverse path establishment process in AODV. [3]

On the other hand, if the intermediate node has a path to the destination node, it will compare the destination sequence number of this path to the destination sequence number in the route request packet. By this way, the intermediate node detects how fresh the path it has to this destination compared to the last path known by the source node. If the path it knows has a greater destination sequence number, it will send a route reply packet to the source. Otherwise the intermediate node behaves as if it has no path to that destination. [3]

Upon receiving the route request, the destination node sends a route reply packet. In turn, this packet traverses the already established reverse route to the source. By receiving the route reply packet, an intermediate node establishes a forward path entry to the node which it has received the reply packet from. This entry indicates that node as the next hop along the forward path to the destination. Then this intermediate node forwards the packet across the reverse path towards the source node.

Figure 4. Shows the process of the forward path establishment in AODV.

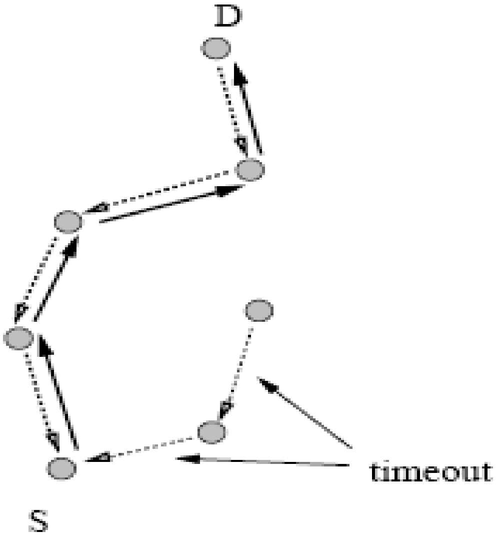

Figure 4. The forward path establishment in AODV. [3]

AODV uses the absence of periodically exchanged beacon packets as an indication to the existence of link breaks. When a link break is detected, the two end nodes of the link send special route reply packets towards the source and the destination across the already established reverse and forward paths, respectively. Consequently, all the nodes on the path ,including the source and the destination, will know about the link break. In turn, the nodes will clean their forwarding entries in both directions along the path. Finally, the source node invokes the route discovery mechanism to find an alternative path.

4 – Location Aided Routing Protocol (LAR)

The most important feature of this protocol is limiting the area of flooding the route request packets in the network. It uses the location information to predict the current location of the destination nodes. LAR assumes the availability of a global positioning system infrastructure (GPS). According to the performance study in [4] LAR schemes introduce less routing overhead than that introduced by the pure flooding schemes. However, it is considered as a two sided solution, as more recourses are required, namely, GPS.

In [4], two LAR schemes are proposed. The first scheme directly employs the concepts of the expected zone and the request zone. In this scheme, namely LAR1, a source node predicts what is called the expected zone of the required destination node. To calculate such prediction, the source node utilizes the location and mobility information about the destination node. LAR schemes depend on GPS to find such information.

The expected zone is defined as a circle. Particularly, the destination node is the centre of that circle. While the radius of that circle defines the expected location prediction error due to GPS errors.

Additionally, the source node defines what is called the request zone. This zone is the largest rectangle which includes both of the current location of the source node and the expected zone of the destination node.

When the source node sends a route request packet to the destination, only the intermediate nodes inside the request zone forward this packet to their neighbors. Other nodes outside the request zone discard the route request packet.

In the second scheme, namely LAR2, the source node uses the available location and mobility information to measure the distance to the expected location of the destination node. Then, it sends a route request packet which includes this distance.

Upon receiving the route request packet, an intermediate node checks if the distance between it and the destination node is less than the distance value included in the route request packet. If it is, the intermediate node will update the packet with its own distance and forward the packet. Otherwise the packet is discarded.

According to [4], LAR1 and LAR2 show similar patterns with respect to the routing overhead, however LAR2 achieves a slightly better performance. But both of them achieve lower routing overhead than that of the pure flooding schemes. This is shown in figure 5.

Form [1, 4], the studies of LAR focuses on the way the protocols forward the route request packets and not the way it maintain the routing information or it reconfigures the broken paths.

5 – Associatively-Based Routing Protocol (ABR)

This protocol has two unique features. The first feature is that ABR uses periodically exchanged beacon packets for two purposes. First ABR uses such packets for detecting the availability of a link. Second it uses them to

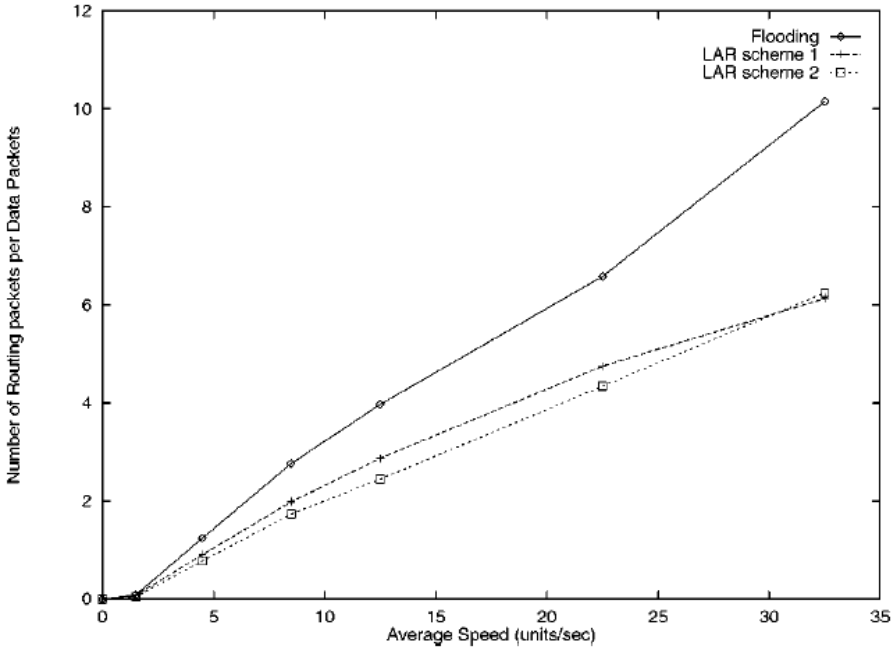

Figure 5. Routing overhead vs. Mobility, A comparing between the two

measure the degree of association between two end nodes of a given link. The later measurement is considered as an indication to the stability of that link. These measurements are used for the route selection process.

Another important feature is that, ABR applies a route maintenance mechanism which is initialized as a local one. However, this mechanism can be expanded to a global one if the local scale is not enough to solve the problem.

Every node in the network expects to periodically receive beacon packets for its neighbors. It keeps a count of the received packets. This count can be used to measure the stability of the link between each two nodes. Consequently, the links in the network are classified as either stable or unstable. This classification is used in the route selection process.

When an intermediate node receives a route request packet from a source, this route request packet contains the path it has traversed to this intermediate node along with the beacon count of each link in the path. According to [5], the route request packet also contains additional information about the neighbor links of the previous intermediate node which has just forwarded this packet to this node.

Consequently, this receiver intermediate node deletes all the additional information in the packet expect that about the link between it and the previous intermediate node. Then it adds its own information about its own adjacent links. Afterwards, this intermediates node forwards the packet directly to all of these links whatever the link is stable or not. [1].

The forwarding process repeats until the packet arrives to the destination node. More than one copy of the request packet may arrive to the destination node which waits for some period of time to allow this to happen. Afterwards, the destination node simply selects the route with the highest record of stable links. And a route reply packet is sent back to the source node.

In case of detecting a link break, the end node of the broken link which is closest to the source node initiates a repair packet with a limited time to live (TTL) [1]. This introduces a local repairing process.

However, if no reply for this packet after some period of time, the procedure is repeated by the previous nodes on the path until a reply is received or half of the length of the path is traversed. The last option is to enforce the source to invoke the route discovery mechanism to establish a completely new route.

ABR gives the stable routes higher preferences that the shortest routes. This is considered as an advantage from the view point of reducing the routing overhead due to route maintenance.

However, the chosen path may be longer than an a less stable but still functional one. This is considered as a main disadvantage of ARB.

6 – Signal Stability-Based Adaptive Routing Protocol (SSA)

The key feature of this protocol is making routing decision based on the signal strength of the links. SSA measures the signal strength of the periodically exchanged beacons between nodes in the network. These measurements are used to classify the links as either stable or unstable.

SSA tries to find a completely stable paths form the beginning, a process that when succeeds to find a path, it will be a very positive side of SSA. On the other hand if this process fails to find a path it may start the entire procedure from the beginning allowing paths with unstable link. This introduces additional effort to find a path. Which is considered as a completely negative side of SSA.

According to [6], SSA consists of two protocols which work together, viz. the forwarding protocol (FP) and the dynamic routing protocol (DRP). When a source node wants to send data packets to a destination node, the FP checks the routing table (RT) of the source node to find any route to this destination. If there is, the packets are directly forwarded, if not the FP initiates a route request packet to find a route.

Upon receiving a route request packet, the DRP on an intermediate node checks the list of the nodes already traversed by the packet to avoid forwarding it in a loop [6]. Then it adds itself to the traversed path and forwards the packet over only stable links [1]. This way, SSA tries to find a completely stable path to the destination node.

But if DRP is not able to find a path to the destination by forwarding the route request packet over stable links; the source node simply floods the network with route request packets which are then forwarded by the intermediate nodes to all links regardless of their stability. However, the intermediate nodes still accept route request packets which are received only through stable links.

The destination node replies the first arriving route request packet, then the source node and each intermediate node along the selected path update their own RTs to reflect the current state of that path. Then the FP can work to forward the packets form the source node to the destination node.

In case of a link break, the two end nodes of the broken link send two special update packets towards both the source and the destination. This way each node on the path can update its own RT to reflect the break status. Then, the source node can invoke the route discovery mechanism to find an alternative route.

7 – Flow-Oriented Routing Protocol (FORP)

The key feature of this protocol is applying a prediction based scheme for selecting and maintaining its routes. It can predict the link expiration time (LET) for a given link. For calculating such predictions, FORP uses information about the current location of the nodes, the velocities and the directions of their movements, and their wireless transmission ranges. For a complete description about how FORP uses such information for its prediction algorithm, please refer to [7]. Consequently, FORP can predict a route expiration time (RET) for a given path. FORP uses such predictions to select the longest likely to live paths and to handoff the current sessions and find alternative paths before the expiration of the currently used ones.

As explained in [7], this scheme allows making routing decisions which ensure some level of quality of service (QoS). Additionally, the performance study in [7] shows the less control overhead required by this class of prediction based protocols. However, a common mobility information source and a common timing reference between the nodes in the networks are required. These requirements of FORP introduce the complexity of depending on other resources, e.g. GPS.

When a source node needs to send packets to a destination node [1, 7]. It first checks its own routing table. If it already has an unexpired path to the destination, it sends the packets directly to the destination. If not, it initiates a route request packet which carries a flow identification number and a sequence number along with the source node address and the destination node address.

Upon receiving the route request message, an intermediate node checks the sequence number in the message. It discards the packet if the sequence number is less than the last received sequence number associated with the flow identification number from this source. In case of equal sequence numbers, the intermediate node forwards the route request message only if it has received it form a path of a larger RET.

Otherwise, the intermediate node adds the LET of the link which it has just received the message from, and adds its address and then it broadcasts the packet. By this way the route request message arrives to the destination node containing the entire traversed path along with its RET. A path is used instead of a currently used one in case if it has a longer RET. [1, 7]

For the route maintenance process, FORP defines a critical time as the difference between the RET of the currently used path and the time the latest packet take to traverse along that path. This time is also affected by the continuously received RET values from the intermediate nodes along with the data packets. When the destination node detect that the critical time is about to be reached, it sends a route hand off packet to the source node. In turn this node initiates the route setup process again. It may select an alternative path based on the received RET values, the number of hops or any other metric included in the route handoff packet.

Summary And Conclusion

A large number of on-demand routing protocols have already been proposed. Each protocol has its own key features, which may add positive or negative sides to the protocol. Generally, on-demand routing protocols share their common ability to adapt with the dynamically changing topology of the wireless ad hoc networks. However, the key disadvantage of these protocols is the introduced delay due to the route discovery and establishment process.

References

[1] C. Siva Ram Murthy and B.S. Manoj. Ad Hoc Wireless Networks: Architectures and Protocols.

[2] Johnson DB, Maltz DA, *“Dynamic source routing in ad-hoc wireless networks”*. In Imielinski T, Korth H (eds). Mobile Computing. Kluwer Academic Publishers: Boston, MA, 1996;

[3] Charles E. Perkins and Elizabeth M. Royer, *“Ad hoc On-Demand Distance Vector Routing. ”*, EEE 1999.

[4] Young-Bae Ko and Nitin H. Vaidya, *“Location-Aided Routing (LAR) in mobile ad*

hoc networks, Proc. of Mobicom, Oct.1998.

[5] Patrick McCarthy, Dan Grigoras, *“Multipath Associativity Based Routing”*, Proceedings of the
WONS 2005, St. Moritz, Switzerland.

[6] R. Dube, C. Rais, K. Wang, and S. Tripathi, “*Signal stability based adaptive routing (ssa) for ad hoc mobile networks,"* February 1997.

[7] William Su and Mario Gerla, “Ipv6 Flow Handoff In Ad Hoc Wireless Networks Using obility Prediction”, IEEE GlobeCom 1999.