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

amr ergawy
aergawy@cc.hu.fi

Abstract:
Wireless Ad hoc networks have it very specific nature of the dynamically changing topology and the relatively limited resources of the transmission medium and the mobile nodes. On demand routing protocols depends on the highly dynamic selecting of routes to adopt with this nature 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 the routing protocols for this class of networks. At the same time, on-demand routing protocols are designed to dynamically adapt with the changes in the topology and the link states of a network. Consequently, on-demand routing protocols always represent a very important candidate to choose for an ad hoc network. However, because the routing overhead required by these protocols to establish a route in response to a request from a source node or to reconfigure a route after a link break, different optimization techniques are required by different protocols to reduce such overhead.

This papers review a group of already proposed on-demand routing protocols. It focuses on the key feature of each protocol, how a protocol establishes routes, and how it reconfigures 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 is a pure on demand protocol, i.e. it does not employ any periodic exchange of packets. DSR does even employ 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, which is considered as the main advantage of DSR [2]. On the hand, DSR employs source routing, so that each data packet contains the full path it should traverse to its destination. Source routing is some time 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 packets is flooded by all intermediate nodes in the network until it arrives to the destination which in turn replies by a route reply packets. The route request packet is initiated with a sequence number which is used by the intermediate nodes to avoid the loop forwarding.

The routing discovery mechanism is optimized by using route caching at the intermediate nodes. To maintain it own cache, each node gathers all possible information from the forwarded packets in the network which contain the whole route to their destinations, since DSR depends on source routing. The nodes may even listen to the traffic which is not directed to them, by working in the promiscuous mode [1]. This way the cache contains what did the node learned about the network. Consequently, an intermediate node may response to a route request packet initiated by a source node if it has a route to the required destination. If a source receives more than one route reply packet, it can choose depending on a defined metric.

The route maintenance mechanism is applied only when some link breaks during a session [2]. Simply the closest node to the source which detects the break sends an update to the source node which in turn invokes the route discovery again to find an alternative route.

3 – Ad Hoc On-Demand Distance-Vector Routing Protocol (AODV):

The key feature of this protocol is that 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, which is considered as an advantage. However this may require additional resources form the intermediate nodes, which is the negative side of AODV. [1].

The route discovery mechanism of AODV may be described as follows. When a node has packets to send to a destination node, it initiates a route request packet. This packet which contains the source address, a sequence number for the source, a sequence number for the destination, a broad cast id and hop count. Each piece of information in this packet has a use in the route setup process. [3]

When a neighbour receives the route request packet it checks from the broadcast Id associated with the source address, if it has received the request before it drops it, other wise it checks if it has a route to the required destination or it does not. If it does not has such route it will build what is called a reverse path entry, and forward the packet to its neighbours. In the reverse path entry, an intermediate node keeps track of which node it has received the route request from; such that when it receives the reply it can forward it back toward the source. The reverse path entry will be deleted after some defined time if no route reply packet is received.

On the other hand, if the intermediate node has a path to the destination node, it will check the destination sequence number of this path to the destination sequence number in the route request packet, which indicates the last value of the destination sequence number known by the source of the route request for the required destination. If it has a greater number, it will send a route reply to the source, other wise it follows the same procedure as it does not has a path. [3]

Upon receiving the route request, the destination sends a route reply packet, which in turn 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 it

receive the reply packet from to indicate it as the next hop in the path. Then this intermediate node forwards the packet across the reverse path towards the source of the route request packet.

When a link break is detected, by the absence of the periodic beacons between its two end nodes, these nodes send a special route reply packets towards along the already established reverse and the forward paths. This way all the nodes on the path including the source know about it, such that they clean their forwarding entries and the source invokes the route discovery mechanism.

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 scheme. 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 uses the location and mobility information which it already has about the destination node to predict what is called the expected zone of the destination. This zone takes the shape of a circle where the destination is the centre and the radius of the zone represented the expected location prediction error due to GPS errors. Then the source defines what is called the request zone. This zone is the largest triangle which includes both of the source node and the expected zone of the destination. When the source node sends the route request packet to the destination, only the intermediate nodes inside the request zone forward this packet to their neighbours, other nodes discard it.

In the second scheme, namely LAR2, the source node uses the available location and mobility information to measure the distance to the expected location destination node. Then, it sends a route request packet which includes this distance. Upon receiving the route request packet, a source 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, it will update the packet with its own distance and forward the packet. Other wise 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.

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. First, it uses periodic beacon packets not just to

detect the availability of a link, but also to measure the associatively with its neighbour through this link, namely, the stability of the link. This criterion is used for the route selection process. Second, it applies a route maintenance mechanism which is initialized as a local one but can expand 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 a neighbour. It keeps a count of the received packets. This count can be used to measure the stability of the link between the 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 traversed to this intermediate node along with the beacon count of each link in the path. Then this According to [5], the route request packet contains also additional information about the neighbour links of the previous intermediate node which has just forwarded this packet to this node. So that, this receiver node deletes all the additional information in the packet expect that of the link between it and the previous node then it adds its own information about its own adjacent links. Then, it forwards the packet directly to all of these links whatever the link is stable or not. [1]. Then the 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 time period to allow this to happen. Afterwards, the destination node simply selects the route with the highest record of stable links.

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.

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

The key feature of this protocol is making the 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 if succeeded 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 procedure form the beginning allowing paths with unstable link, which means additional effort to find a path.

According to [6], SSA consists of two protocols which are working together, viz. the forwarding protocol (FP) and the dynamic routing protocol (DRP). When a source wants to send data packets to a destination, the FP checks the routing table (RT) of the source node to find any route to this destination. If it has a route 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 and forwards the packet over only stable links [1]. This way, SSA tries to fine a completely stable path to the destination. But DRP is not able to find a path to the destination by forwarding over a stable link; 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, still the accepted route request packets are those received to the intermediate nodes 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 it own RT to reflect the current state of that path. Then the FP can work to forward the packets form the source to the destination.

In case of a link break, the two ends 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 and 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 a complete description about used the prediction algorithm, refer to [7], and consequently it 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 timing reference between the nodes in the networks is required which is again introduces the complexity of depending on another resource, namely, GPS.

When a source node needs to send packets to a destination node [1, 7]. First, it checks its own routing table. If it already has an unexpired path to the destination, it sends the packet 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, and then 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 it received the message form, and adds its address and then it broadcasts the packet. This way the route request message arrives to the destination node continuing the entire traversed path

along with its RET. A path is used instead of a currently used one in case of it has a longer RET. [1, 7]

For the route maintenance process, FORP defines a critical as the difference between the RET of the currently used path and the time the latest packet take to traverse along the path. This time is also affected by the continuously received RET values form 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 route which initiates the route setup process again based on the RET values, the number of hops or any other information included in the route handoff packet.

Summery 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. However, on-demand routing protocols share their common ability to adopt with the dynamically changing topology of the wireless ad hoc networks, in spite of the delay required to find routes to destination nodes.

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 Mobility Prediction", IEEE GlobeCom 1999.