A Qualitative Comparison of Position-Based Routing Protocols for Ad-Hoc Networks

Liana Khamis Qabajeh[1] **Dr. Miss Laiha Mat Kiah**[2] **Mohammad Moustafa Qabajeh**[3]

[1,2]Faculty of Computer Science and Information Technology, University of Malaya, Malaysia
[3]Department of Electrical and Computer Engineering, IIUM, Malaysia

Summary
Wireless Ad-Hoc networks are collection of nodes that can communicate without any fixed infrastructure. A crucial problem in Ad-Hoc networks is finding an efficient route between a source and a destination. The need for scalable and energy efficient protocols, along with the recent availability of small, inexpensive and low power positioning instruments justify introducing position based routing algorithms in mobile Ad-Hoc networks.
This paper presents an overview and a qualitative comparison of the existing Ad-Hoc routing protocols that make forwarding decisions based on the geographical position of a packet's destination. We conclude our findings by investigating opportunities for future research.
Key words:
position-based routing, location-aware routing, ad-hoc networks, wireless networks.

1. Introduction

Ad-Hoc wireless networks are self-organizing multi-hop wireless networks, where all the hosts take part in the process of forwarding packets. Ad-Hoc networks are highly applicable in many fields, such as emergency deployments and community networking. A fundamental and challengeable task in Ad-Hoc wireless network is an efficient routing protocol since all the nodes in the network act as hosts as well as routers.
Many routing protocols those are compatible with the characteristics of Ad-Hoc networks have been proposed. In general, they can be divided into two main categories: ***topology-based*** and ***position-based***. ***Topology-based*** routing protocols use information about links that exist in the network to perform packet forwarding. They are, in turn, divided into three categories: ***proactive***, ***reactive*** and ***hybrid*** (hierarchical) protocols.
Proactive routing protocols periodically broadcast control messages in an attempt to have each node always know a current route to all destinations. It is obvious that proactive routing protocols are less suitable for Ad-Hoc wireless networks because they constantly consume power throughout the network, regardless of the presence of network activity.
On the other hand, ***reactive*** routing protocols are deemed more appropriate for wireless environments because they initiate a route discovery process only when data packets need to be routed. One advantage of reactive routing protocols is that no periodic routing packets are required. However, they may have poor performance in terms of control overhead in networks with high mobility and heavy traffic loads. Scalability is said to be another disadvantage because they rely on blind broadcasts to discover routes.
As seen, proactive routing uses excess bandwidth to maintain routing information, while reactive routing involves long route request delays and floods the entire network for route determination. ***Hybrid*** routing protocols aim to address these problems by combining the best properties of both approaches. In general, topology-based are considered not to scale in networks with more than several hundred nodes [1].
In recent developments, ***position-based*** routing protocols exhibit better scalability, performance and robustness against frequent topological changes. Position-based routing protocols use the geographical position of nodes to make routing decisions, which results in improving efficiency and performance. These protocols require that a node be able to obtain its own geographical position and the geographical position of the destination. Generally, this information is obtained via Global Positioning System (GPS) and location services.
There are three main packet-forwarding strategies used for position-based protocols: ***greedy forwarding***, ***restricted directional flooding*** and ***hierarchical*** approaches. ***Greedy forwarding*** protocols do not establish and maintain paths from source to the destination, instead, a source node includes the approximate position of the recipient in the data packet and selects the next hop depending on the optimization criteria of the algorithm; the closest neighbor to the destination for example. Similarly, each intermediate node selects a next hop node until the packet reaches the destination. In order for the nodes to be enable to do this, they periodically broadcast small packets

Manuscript received February 5, 2009
Manuscript revised February 20, 2009

(called beacons) to announce their position and enable other nodes maintain a one-hop neighbor table. Such an approach is scalable and resilient to topology changes since it does not need routing discovery and maintenance; however, periodic beaconing creates lot of congestion in the network and consumes nodes' energy.

While the beaconing frequency can be adapted to the degree of mobility, a fundamental problem of inaccurate (outdated) position information always presents: a neighbor selected as a next hop may no longer be in transmission range. This leads to a significant decrease in the packet delivery rate with increasing node mobility. To reduce the inaccuracy of position information, it is possible to increase the beaconing frequency. However, this also increases the load on the network by creating lot of congestion, increasing the probability of collision with data packets and consuming nodes' energy [1, 2].

Unfortunately, greedy routing may not always find the optimum route, even it may fail to find a path between source and destination when one exists [3, 4]. An example of this problem is shown in Fig.1. The circle around S shows the transmission range of S. Note that there is a valid path from S to D. The problem here is that S is closer to the destination D than any of the nodes in its transmission range; therefore greedy forwarding will reach a local maximum from which it cannot recover. Generally, greedy forwarding works well in dense networks, but in sparse networks it fails due to voids (regions without nodes) [2].

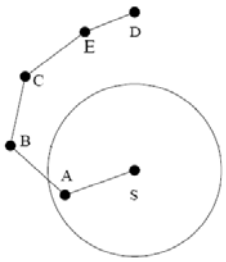

Fig.1 Greedy routing failure example.

In ***restricted directional flooding***, the sender broadcasts the packet (whether the data packet or route request packet) to all single hop neighbors towards the destination. The node which receives the packet, checks whether it is within the set of nodes that should forward the packet (according to the used criteria). If yes, it will retransmit the packet. Otherwise, the packet will be dropped.

In restricted directional flooding, instead of selecting a single node as the next hop, several nodes participate in forwarding the packet in order to increase the probability of finding the shortest path and be robust against the failure of individual nodes and position inaccuracy.

The third forwarding strategy is to form a ***hierarchy*** in order to scale to a large number of mobile nodes. Some strategies combine nodes location and hierarchical network structures by using the zone based routing. Others use the dominating set routing. Some others present a two level hierarchy within them; if the destination is close to the sender (in number of hops), packets will be routed base on a proactive distance vector. Greedy routing is used in long distance routing.

This paper gives an overview of existing position-based routing protocols for mobile Ad-Hoc networks. We outlined the main problems that have to be solved for this class of routing protocols and presented the solutions that are currently available.

The protocols that have been selected for analysis are MFR [5], I-PBBLR [1], DREAM [6], LAR [7], GRID [8], TERMINODES [9], LABAR [10], SPAAR [11], and AODPR [12]. It worth nothing that many other position-based routing protocols exists for mobile Ad-Hoc networks; however, we have selected what we regard as representative for the existing approaches.

The rest of the paper is organized as follows. Section 2 gives an overview of the selected position-based routing protocols. Section 3 contains a qualitative comparison of the discussed protocols. Directions of future research are discussed in section 4. Finally, we conclude the paper in Section 5.

2. Overview of Selected Position-Based Routing Protocols

In this section the selected protocols are described. For each protocol, we tried to summarize its main objectives, how it works and its advantages and disadvantages compared to other protocols.

2.1 MFR

Some greedy position-based routing protocols, such as *Most Forward within distance R (MFR)* [5], try to minimize the number of hops by selecting the node with the largest progress from the neighbors. Where progress is defined as the projection of the distance of the next hop from the sender on the straight line between the sender and the destination. In Fig.2, if the MFR is used the source S will choose the node A as the next hop since it has the largest progress to the destination D.

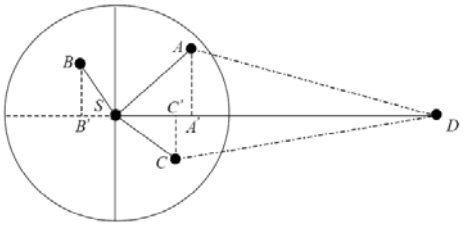

Fig.2 MFR example.

As other greedy forwarding protocols, *MFR* has the shortcomings of either not guaranteeing to find a path to the destination or finding a path which is much longer than the shortest path. Moreover nodes periodically should broadcast beacons to announce their positions and enable other nodes maintain a one-hop neighbor table.
MFR is the only progress-based algorithm competitive in terms of hop count [13]. However, choosing the node with the largest progress as the next hop will increase the probability that the two nodes disconnected from each other before the packet reaches the next hop. So, the packet drop rate increases greatly, especially in highly mobile environments. Such a situation is very common due to neighbor table inconsistency [2].

2.2 I-PBBLR

Most position-based routing protocols use forwarding strategies based on distance, progress or direction. *Improved progress Position Based BeaconLess Routing algorithm (I-PBBLR)* [1] combines the traditional progress with the direction metric to form the improved progress definition. The authors have chosen the cosine of the angle since its value is between 0 and 1, and it is even. If the traditional progress is multiplied by the cosine of the angle, both the minimum and maximum of the progress are not changed. Also, it fits for the need that the node has smaller angle will forward packet earlier.
I-PBBLR tries to eliminate the beaconing drawbacks by using a beaconless protocol. In beaconless protocols the sender makes non-deterministic routing decisions, implicitly allowing opportune receiving nodes to determine a packet's next-hop through contention at transmission time. In I-PBBLR, if a source node has a data packet to send, it first determines the position of the destination, stores these geographical coordinates along with its own current position in the header of the packet, and broadcast the packet to all neighboring nodes (since it does not possess knowledge of neighboring nodes positions).
Nodes located within the forwarding area of the relaying node, apply Dynamic Forwarding Delay (DFD) prior to relaying the packet, whereas nodes outside this area drop the received packet. The value of the DFD depends on the relative position coordinates of current, previous and destination node. Eventually, the node that computes the shortest DFD forwards the packet first by broadcasting it to all neighboring nodes after replacing the previous node's position by its current position in the header). Every node in the forwarding area detects the further relaying of the packet and cancels its scheduled transmission of the same packet. This mechanism allows selecting one neighbor as next hop in a completely distributed manner without having knowledge of the neighboring nodes, which is achieved by applying the concept of DFD. The simulation results showed that position based beaconless routing using the improved progress reduced the overhead and increased delivery rate by 3-5% compared with using the traditional progress.

2.3 DREAM

Distance Routing Effect Algorithm for Mobility (DREAM) [6] is an example of restricted directional flooding routing protocols, that within them, the sender will broadcast the packet towards nodes in a limited sector of the network; to all single hop neighbors towards the destination. DREAM algorithm is a proactive protocol that uses a limited flooding of location update messages [13]. In DREAM, each node maintains a position database that stores position information about all other nodes in the network. Its location service can therefore be classified as an all-for-all approach. Thus, each node regularly floods packets to update the position information maintained by the other nodes. The higher the speed of a node the more the frequency with which it sends position updates. Also, the distance that a position update may travel before it is discarded provides accurate position information in the direct neighborhood of a node and less accurate information at nodes farther away, but this does not cause a problem since intermediate hops are able to update the position information contained in the data packet. In DREAM the message is forwarded to all neighbors whose direction belongs to the region that is likely to contain the destination D, called the expected region. Expected region is determined by the tangents from the source S to the circle centered at D and with radius equal to a maximal possible movement of D since the last location update. The neighboring hops repeat this procedure using their information on D's position.
Fig.3 gives an example for the expected region in DREAM. If a node does not have a one-hop neighbor in the required direction, a recovery procedure has to be started. However, this procedure is not part of the DREAM specification [3].

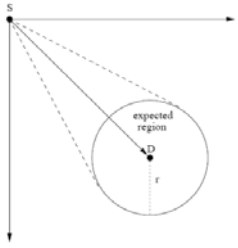

Fig.3 Example of the expected region in DREAM.

Since DREAM uses the restricted directional flooding to forward data packets themselves, there will be multiple copies of each packet at the same time. This increases the probability of using the optimal path; however, it

decreases its scalability to large networks with a high volume of data transmissions and makes it more suitable for applications that require a high reliability and fast message delivery for infrequent data transmissions.

2.4 LAR

Like DREAM, *Location-Aided Routing (LAR)* [7] is an example of restricted directional flooding routing protocols; however, partial flooding is used in LAR for path discovery purpose and in DREAM for packet forwarding. Hence, LAR proposes the use of position information to enhance the route discovery phase of reactive Ad-Hoc routing approaches. The expected zone is fixed from the source and defined based on the available position information (e.g., from a route that was established earlier). A request zone is defined as the set of nodes that should forward the route discovery packet. The request zone typically includes the expected zone. Two request zone schemes have been proposed in. The first scheme is a rectangular geographic region. In this case, nodes will forward the route discovery packet only if they are within that specific region. This type of request zone is shown in Fig.4.

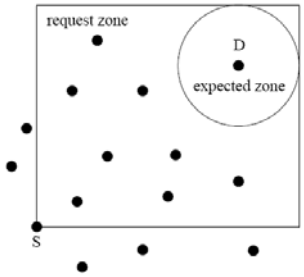

Fig.4 Example of request and expected zones in scheme 1 of LAR.

In LAR scheme 2, the source or an intermediate node will forward the message to all nodes that are closer to the destination than itself. Thus, the node that receives the route request message will check if it is closer to the destination than the previous hop it will retransmit the route request message; otherwise, it will drop the message. In order to find the shortest path in the network level, instead of selecting a single node as the next hop, several nodes will be selected for managing the route request message and each of them will put its IP address in the header of the request packet. Therefore, the route through which the route request message is passed will be saved in the header of the message; message size will grow as it goes far from the source and the routing overhead will be increased.

2.5GRID

In *GRID* algorithm [8] the dominating set concept is applied. A set is dominating if all the nodes in the system are either in the set or neighbors of nodes in the set. Routing based on a connected dominating set is a promising approach, since the searching space for a route is reduced to nodes in the set. GRID tries to exploit location information in route discovery, packet relay and route maintenance. In GRID the geographic area is partitioned into a number of squares called grids. In each grid, one mobile host (the one nearest to the physical center of the grid) will be elected as the leader of the grid. The size of each grid depends on transmission radius *R*, and several options are proposed, with general idea of one leader being able to communicate directly with leaders in neighboring grids, and all nodes within each grid being connected to their leaders. Routing is then performed in a grid-by-grid manner through grid leaders, and non-leaders have no such responsibility. Hence, the number of packets related to route search is insensitive to the network density. On the contrary the cost slightly goes down as the host density increases, since routes are becoming more stable with denser hosts.

In GRID efforts are made in two directions to reduce the route search cost; using the locations of source and destination to confine the search range (like request zone in LAR) and delegating the searching responsibility to the gateway hosts. One attractive feature of GRID is its strong route maintenance capability since when a leader moves, another leader from the same grid replaces it by a handoff procedure. The probability of route breakage due to a nodes roaming is reduced since the next hop is identified by its physical location, instead of its address. Grid uses a specific field to detect duplicate request packets from the same source, so endless flooding of the same request can be avoided.

The simulations in [8] showed that GRID can reduce the probability of route breakage, reduce the number of route discovery packets and lengthen routes' lifetime. On the other hand their simulations showed that GRID uses longer paths than that used with LAR, since the former always confines relay hosts to gateway hosts while LAR tries to search the route with the smallest host count. Also, the authors do not elaborate on route maintenance required when a grid remains empty after its leader and only node leaves it [13]. Finally, developing protocols that have as many as possible sleeping nodes, such as GRID, will save network energy significantly.

2.6 TERMINODES

TERMINODES [9] is an example of hierarchical routing protocols. TERMINODES presents a two level hierarchy within which, if the destination is close to the sender (in terms of number of hops), packets will be routed base on a proactive distance vector. Greedy routing is used in long distance routing. TERMINODES addresses the following

objectives: scalability (both in terms of the number of nodes and geographical coverage), robustness, collaboration and simplicity of the nodes [13].

This routing scheme is a combination of two protocols called Terminode Local Routing (*TLR*) and Terminode Remote Routing (*TRR*). *TLR* is a mechanism that allows to reaching destinations in the vicinity of a terminode and does not use location information for making packet forwarding decisions. *TRR* is used to send data to remote destinations and uses geographic information; it is the key element for achieving scalability and reduced dependence on intermediate systems. The major novelty is the Anchored Geodesic Packet Forwarding (*AGPF*) component of *TRR*. This is a source path based method designed to be robust for mobile networks: Instead of using traditional source paths, that is lists of nodes, it uses anchored paths. An anchored path is a list of fixed geographical points, called anchor. The packet loosely follows anchored path. At any point, the packet is sent in the direction of the next anchor in the anchored path by applying geodesic packet forwarding. When a terminode finds that the next anchor geographically falls within its transmission range, it deletes it from the anchored path and sends in the direction of the new next anchor. This is repeated until the packet is sent in direction of the final destination [13].

The authors of [9] showed by means of simulations for mobile Ad-Hoc networks composed of several hundreds of terminodes, that the introduction of a hierarchy can significantly improve the ratio of successfully delivered packets and the routing overhead compared to reactive Ad-Hoc routing algorithms. They also demonstrated benefits of the combination of *TLR* and *TRR* over an existing protocol that uses geographical information for packet forwarding. However, using greedy routing in long distance routing makes TERMINODES inherits the problems associated with it.

2.7 LABAR

Location Area Based Ad-Hoc Routing for GPS-Scarce Wide-Area Ad-Hoc Networks **(***LABAR)* [10] is a hybrid virtual backbone and geographical location area based Ad-Hoc routing. Authors outlined that using GPS can increase the cost and power consumption of small mobile nodes. Thus, LABAR requires only a subset of nodes (G-nodes) to know their exact location forming location areas around them. G-nodes are interconnected into a virtual backbone structure to enable efficient exchange of information for the mapping of IP addresses to locations. Nodes that are not enabled with GPS equipment are called S-nodes.

Routing in LABAR consists mainly of three steps: zone formation, virtual backbone formation and directional routing. The first step of LABAR deals with forming the zones, i.e., making the decision on which S-nodes should belong to which G-nodes. It was assumed that all G-nodes start the zone formation algorithm at the same time to acquire S-nodes. If an S-node has already been attached to a G-node then the request message is ignored by the S-node. Upon including a S-node in a zone, it initiates the zone formation algorithm on its own to draw more S-nodes form its neighborhood into its zone. By the end of this step, all S-nodes will belong to a G-node and G-nodes will know the IDs of their zone's S-nodes. The second step is creating an easy to manage virtual backbone for relaying position information of nodes. G-nodes in the virtual backbone are responsible for resolving the IP addresses into geographical locations. To connect zones and get the virtual backbone to function, a G-node called the root sends connect messages to its adjacent zones. If the particular adjacent zone is not connected yet to the backbone, then it will be added to the backbone. Fig.5 shows an example of such a virtual backbone.

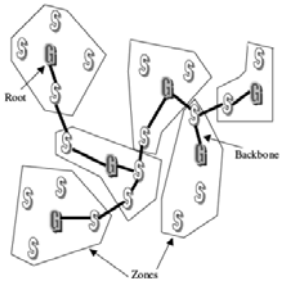

Fig.5 Example of virtual backbone in LABAR.

The last step is the directional routing. The source node queries the source G-node node to map the destination IP address into the geographical location area of the destination. Then the source G-node determines the vector pointing from its own location to the destination's location. The resulting vector's direction is compared to each of the adjacent zones' direction and distance to determine the neighboring zone that will be used in relaying the data to the destination. Now, the source G-node will instruct the source node on how to route the packet inside the zone to reach the next zone with the least number of hops. The node that received the packet in the neighboring zone will route the packet to the next zone by consulting its zone's G-node (which will consume time). In the case of a failure in the directional route (determined for example through expired hop counters), the source zone will be informed about the failure and the virtual backbone will be used to relay the packets.

Thus, LABAR is a combination of proactive and reactive protocols, since a virtual backbone structure is used to update location information between Gnodes (in a proactive manner), while user packets are relayed using directional routing towards the direction zone of the destination. One of the most important advantages of

LABAR is the reduction of cost and power consumption by the relaxation of the GPS-equipment requirement in each node.

2.8 SPAAR

All the previously mentioned position-based routing protocols are vulnerable to some attacks, as they focus on improving performance while disregarding security issues [12]. In addition most of them are not guaranteed to find the shortest path. In the last few years, a limited work has been done to introduce some security issues to position-based routing protocols. Examples of these are *Secure Position Aided Ad-Hoc Routing (SPAAR*) [11] and *Anonymous On-Demand Position-based Routing in Mobile Ad-Hoc Networks (AODPR)* [12].

SPAAR uses position information in order to improve the efficiency and security of mobile Ad-Hoc networks. It was designed for protecting position information in managed-hostile environment where security is a primary concern and uses geographical information to make forwarding decisions, resulting in a significant reduction in the number of routing messages. It uses asymmetric cryptography to protect against malicious nodes (unauthorized nodes that attempt to disrupt the network) and attempts to minimize the potential for damage of attacks from compromised nodes (authorized nodes those have been overtaken by an adversary). When a node sends a multi-hop message, like a route request or a route reply, this message must be signed with its private key and encrypted with the public key of a neighbor. Every node can verify that the message was sent by a one-hop neighbor, and the destination can also verify that the sender is who it claims to be.

SPAAR achieves a high level of security by allowing nodes to only accept routing messages from one-hop neighbors. This is done to prevent the invisible node attack and the wormhole attack. To participate in SPAAR, each node requires a public/private key pair, a certificate binding its identity to its public key (signed by a trusted certificate server), and the public key of the trusted certificate server. Each node periodically broadcasts a "table update" message to inform the neighbors of its new position coordinates and transmission range. Each node maintains a neighbor table that contains the identity and position information of each verified neighbor, along with the cryptographic keys required for secure communication with each neighbor; the used location service is all-for-some.

In addition to the neighbor table, each node maintains another one for the recent destinations it has communicated with. The tables are very similar, except that the destination table also contains information about the speed of the node, making it possible to predict the next position of the node. If this is the source node's first attempt at communication with a particular destination, the source may not have the destinations position. In this situation, a location service may be used. If no location service is available, a selective flooding algorithm may be used to reach the destination and receive its position information.

To find a route to a specific destination, the source broadcasts a Route REQuest (RREQ) encrypted with its group encryption key. An intermediate node checks to see if it, or any of its neighbors, is closer to destination it forwards the RREQ else the RREQ is dropped. Intermediate nodes record in their route cache the address of the neighbor from which they received the RREQ, thereby establishing a reverse path. This process is repeated until the destination is reached. Upon receiving a RREQ, the destination constructs a Route REPly (RREP) signed with its private key and encrypted with the public key of the neighbor it received the RREQ from. The RREP propagates along the reverse path of the RREQ, being verified at each hop.

The fact that SPAAR makes use of geographic routing helps reducing the overall overhead. It is also very efficient when talking about security issues; however, it requires the double of processing time, since it uses asymmetric cryptography, not only for end to end communication, but also for hop-to-hop communications [30]. SPAAR has a centralized trust and so suffer from the compromised server problem and the single point of failure.

2.9 AODPR

Mobile Ad-Hoc networks are susceptible to malicious traffic analysis and many attacks due to the infrastructure-less, dynamic and broadcast nature of radio transmissions. One of these attacks is the target-oriented attack which is determining a target node and conducting an intensive attack against it. In [12] *Anonymous On-Demand Position-based Routing in Mobile Ad-Hoc Networks (AODPR)* was proposed while these two problems in mind. It keeps routing nodes anonymous, thereby preventing possible traffic analysis. A time variant Temporary IDentifier (Temp ID) is computed from time and position of a node and used for keeping the node anonymous. Moreover, AODPR uses the concept of Virtual Home Regions (VHR) [4] which is a geographical region around a fixed center. In this scheme each node stays in one of the VHRs and nodes within a VHR obtain their own geographic position through GPS and report their position information to the Position Servers (PS). PSs are trusted Ad-Hoc nodes distributed in the network. The PS keeps the position information of the nodes securely. When a node joins the network, it makes its registration to the PS and gets a

common key and a pair of public and private keys from the PS [12].

When a node wants to get position information of other nodes, it first authenticates itself to the PS and sends a signed position request, and then PS provides it with the required position information, Public Key of the destination and other needed information. The source, before sending the route request, estimates Temp NH, which is initially the minimum number of hop which the route request packet travels to find a route from the source to the destination. Each intermediate node (Forwarder) updates Temp NH, Temp NH = Temp NH - 1, and compares the updated Temp NH with the minimum number of hop which route request packet travels to find a route from this node to the destination (h'). If h' is less than or equal to Temp NH, then forwarder forwards the packet to its radio region and keeps the route information, else it discards the packets. Both h' and NH are calculated depending on the distance from the node to the destination and the radius of the maximum radio range coverage of each node. At the last phase of the route discovery procedure, the destination replies with a route reply message signed with its private key. The analysis in [12] shows that AODPR ensures the anonymity of route as well as nodes, the robustness against the target-oriented attack and several others, and it is applicable to any node density in a Network. However, many fields such as NH and destination position taken from PSs are encrypted using the Common key (CK); if this key is compromised a large percentage of the communication in the whole network will be compromised. AODPR suffers from two problems inherited from the VHR approach it uses. First, nodes can be hashed to a distant VHR, leading to increased communication and time complexity, as well as problems if the VHR of a node cannot be reached. Second, since an Ad-Hoc network is dynamic, it might be difficult to guarantee that at least one position server will be present in a given Ad-Hoc network [3].

3. Comparison of selected protocols

Table.1 summarizes the discussed protocols together with the evaluation criteria used. This summary is a high level qualitative comparison of the protocols rather than a precise quantitative performance evaluation. The following is an explanation of the criteria used for comparison:

- Forwarding strategy type: describes the fundamental strategy used for packet forwarding.
- Robustness: the robustness of an approach is considered to be high if the failure (or absence due to mobility) of a single intermediate node does not prevent the packet from reaching its destination. It is medium if the failure of a single intermediate node might lead to the loss of the packet but does not require the set up of a new route. Finally, the robustness is low if the failure of an individual node might result in packet loss and the setting up of a new route. According to this definition, the routing protocols that begin data transmission immediately without the need for routing setup have at least medium robustness.
- Implementation complexity: describes how complex it is to implement and test a given forwarding strategy. This measure is highly subjective and we will explain our opinion while discussing each protocol.
- Scalability: describes the performance of the protocol with increasing number of nodes in the network. It can be classified as follows: high scalability is used when a network grows as much as it needs and the approach is still able to maintain a good performance. Medium scalability means that an approach can handle networks with a reasonable size, but may have problems if it grows. Low scalability describes protocols which restrict to small networks. Since all the position-based routing protocols are scalable, all the discussed protocols have at least medium scalability.
- Packet overhead: refers to bandwidth consumption due to larger packets and/or higher number of signaling packets. The protocols can be classified as follows: Low overhead is used to describe protocols which have small packets and reduce the number of packets sent using unicast for example. Medium overhead is used to classify the protocols that have small packets but require large number of signaling packets, or if they require larger packets but use unicast to send the data. High overhead means that an approach requires larger packets as well as an increased number of signaling packets. Note that all the position-based routing protocols have lower packet overhead compared to other types, but this criterion is defined to compare the position-based routing protocols together.
- Processing overhead: is used to associate each protocol with processing requirements. Low processing refers to approaches that require a low CPU processing, such as unsecure protocols. Medium processing will be used to classify the secured protocols. High processing is used to describe protocols that use multiple security techniques together.

MFR, as a greedy forwarding protocol is both efficient and very well suited for use in Ad-Hoc networks with a highly dynamic topology [3]. Its robustness is medium since the failure of an individual node may cause the loss of a packet in transit, but it does not require setting up a new route, as would be the case in topology-based Ad-Hoc routing. Such an approach is very easy to implement and scalable since it does not need routing discovery and maintenance. Moreover, it has a low packet and

processing overhead because of its few number of small-size packets compared to other secure position based protocols.

Table.1 Characteristics of the presented forwarding strategies

Metric	*Type*	*Robustness*	*Implement. Complexity*	*Scalability*	*Packet Overhead*	*Processing Overhead*
MFR	Greedy (progress)	Medium	Low	High	Low	Low
I-PBBLR	Greedy (progress +direction)	Medium	Low	High	Low	Low
DREAM	Restricted Directional Flooding	High	Low	Medium	Medium	Low
LAR	Restricted Directional Flooding	Low	Low	Medium	Medium	Low
Grid	Hierarchical	Medium	Medium	High	Low	Low
TERMINODES	Hierarchical	Medium	Medium	High	Low	Low
LABAR	Hierarchical	High	Medium	High	Low	Low
SPAAR	Restricted Directional Flooding	Low	High	Medium	High	High
AODPR	Restricted Directional Flooding	Low	Medium	Medium	Medium	Medium

I-PBBLR inherited all the properties of greedy forwarding; however, using a beaconless protocol slightly increases the robustness and scalability, reduces the packet overhead, and improves the performance in sparse networks compared to traditional greedy protocols.

Restricted directional flooding protocols, such as ***DREAM*** and ***LAR***, are robust against position inaccuracy since they use the expected region concept. They have higher communication complexity than greedy ones and therefore have less scalability to large networks; their scalability and packet overhead are considered to be medium. However their processing overhead is low due to non-secure routing. Also, they are very simple to be implemented.

DREAM's requires all nodes maintain position information about every other node. This leads to large overhead due to position update and large position information maintained by each node. On the other hand, a position query requires only a local lookup LAR however, just uses the available position information from a route that was established earlier.

DREAM is very robust against the failure of individual nodes since the data packet goes through multiple paths, so the failure of a single intermediate node does not prevent the packet from reaching its destination. This qualifies it for applications that require a high reliability and fast message delivery for very infrequent data transmissions [3]. LAR is robust during the route discovery since the RDP packet goes through multiple paths; however, after route setup it is like any other protocols that depend on route setup before sending the data packets, i.e., the failure of a single node might result in packet loss and the setting up of a new route. Hence, its robustness is considered to be low. On the other hand establishing a route before beginning data sending makes it more suitable than DREAM in the cases that requires high volume of data transmissions.

Although ***Grid*** has strong route maintenance capability and it is very robust towards node mobility, it is like any other protocol that depends on route setup before sending the data packets in the sense that the failure of a single node might result in packet loss and the setting up of a new route. Moreover, the authors in [8] did not elaborate on route maintenance required when a grid remains empty after its leader and only node leaves it [13]. Thus, its robustness is considered to be medium. Grid's implementation complexity is considered to be medium due to dealing with the area as grids. Its scalability is high due to using restricted directional flooding and delegating the searching responsibility to the gateway hosts. Its packet and processing overheads are considered to be low due to reduced number of small non-secure routing packets.

TERMINODES robustness is medium since the failure of an individual node may cause the loss of a packet in transit, but it does not require setting up a new route, as would be the case in topology-based Ad-Hoc routing. Due to using the two level hierarchy approach, TERMINODES is considered to have medium implementation complexity. Such an approach is scalable since it does not need routing discovery and maintenance in long distance routing. Moreover, it has a low packet and processing overhead because of its few number of small-size packets compared to other secure position based protocols.

LABAR exhibits some properties of greedy forwarding such as high scalability and low packet overhead. In the case of a failure in the directional route of LABAR the virtual backbone will be used to relay the packets, i.e., LABAR's robustness is high since a failure of a single intermediate node does not prevent the packet from reaching its destination. LABAR's implementation complexity is considered to be medium due to using zones and its processing overhead is low due to non secure routing.

SPAAR's robustness is low since the failure of an individual node might result in packet loss and the setting up of a new route. It has high implementation complexity since messages must be verified, signed with the private key and encrypted with the public key of a neighbor.

SPAAR assumes the existence of one certificate server, which may be the operation bottleneck specially in large area networks. Moreover, increasing the number of nodes

in the network with using the restricted directional flooding will increase the packet overhead. Finally, in large area networks the probability of having long routes will increase, and since each node spends time in signing and encrypting the messages, the probability of node movements and route breakage will increase. For these three reasons SPAAR is considered to have a medium scalability. Moreover, SPAAR has a high packet overhead because of the large-size packets due to the security techniques used and increased number of packets compared to greedy forwarding. These security techniques lead also to high processing overhead.

The robustness of ***AODPR*** is considered as low since the failure of an individual node might result in packet loss and the setting up of a new route. AODPR's implementation complexity is considered to be medium since messages are signed only with the private key of each node. So its complexity is less than SPAAR since it does not use neighbor public key. AODPR has a medium scalability since increasing the number of nodes in the network with the usage of the restricted directional flooding will increase the packet overhead. However, it still has a higher scalability than SPAAR due to the reasons mentioned in the discussion of SRAAR scalability. AODPR also has a less packet overhead compared to SRAAR. Even though the number of sent packets in AODPR is large, its packet size is smaller than that in SPAAR due to the later security techniques; AODPR is considered to have a medium packet overhead and processing overhead.

4. Directions of Future Research

In this paper we have shown that there are many approaches to perform position-based packet forwarding. However, there still exist a number of issues and problems that need to be addressed in future research.

Position-based protocols make it possible to have larger networks without scalability problems. However, geographical routing also offers attackers new opportunities specially that most protocols broadcast position information in the clear allowing anyone within range to receive. Hence, node position can be altered, making other nodes believe that it is in a different position. This may make nodes believe that the attacker is the closest node to the destination and choose it as the next hop. Consequently, this attacker will be able to alter or drop packets. Thus, it is worth that more intensive work be done to secure position-based routing protocols to be able to defend against several attacks not only from malicious nodes, but also from the compromised ones. Additionally, location privacy is one of the most major issues that need to be addressed, since location privacy is hard to achieve when a node identifier can be immediately associated with its position.

Geographical routing protocols depend strongly on the existence of distributed scalable location services, which are able to provide the location of any host at any time throughout the entire network. Hence, researches should consider the scalability point upon developing new location services. Also, the most common way to enable nodes of knowing their locations is by equipping them with GPS. To decrease the cost and power consumption of small mobile nodes other techniques for finding relative coordinates should be discussed.

We also need more concentration on power aware routing for saving network energy by developing protocols that have as many as possible sleeping nodes and designing sleep period schedules for each node. Also, more studies should concentrate on Quality of Service (QoS) position based routing and multicast position based routing.

Most routing protocols (not only position-based) consider nodes as neighbors if the Euclidean distance between them is at most equals the transmission radius which is the same for all nodes in the network. However, irregular transmission radius of a node (due to obstacles or noise), unidirectional links and different nodes' transmission radii should be taken into consideration. Moreover, many applications have nodes distributed in three-dimensional space and few researches have been done yet in this field.

Another issue that needs to be addressed is enabling the connectivity among the individual Ad-Hoc networks, as well as connectivity of any given Ad-Hoc network to the Internet. This will, most likely, require the usage of hierarchal approaches to achieve scalability. This field has been already begun; however, it needs further investigation.

5. Summary and Conclusions

Efficient routing among a set of mobile hosts is one of the most important functions in Ad-Hoc wireless networks. This paper has presented the current state of position-based Ad-Hoc routing and provided a qualitative evaluation of the presented approaches. At the end, we identified a number of research opportunities which could lead to further improvements in position-based Ad-Hoc routing.

Forwarding techniques based on position information was classified into three distinct categories. Greedy routing does not require the maintenance of explicit routes; however, it works by forwarding a single copy of data packet towards the destination. If a local maximum is encountered, a repair strategy can be used to avoid dropping the packet. The greedy packet forwarding is an efficient approach that scales well even with highly dynamic networks, and it is a promising strategy for

general purpose position-based routing. However, it is not guaranteed to find the optimal path.

In restricted directional flooding the packets are broadcasted in the general direction of the destination. Restricted directional flooding has higher packet overhead and less salability. However, its opportunity to find the shortest path is higher.

Using hierarchical approaches increase the approach scalability. This may be done through the usage of zone based routing, dominating sets, or by means of a position-independent protocol at the local level and a greedy variant at the long-distance level.

Security has recently gained a lot of attentions in topology-based routing protocols and many attempts in proposing end-to-end security schemes have been done. However, it is obvious from the analysis that a few research efforts have addressed position-based security issues.

References

[1] Cao, Y., Xie, S. (2005). A Position Based Beaconless Routing Algorithm for Mobile Ad hoc Networks. Proceedings of the International Conference on Communications, Circuits and Systems, 1(1), 303-307, IEEE.

[2] Giruka, V., Singhal, M. (2005). Angular Routing Protocol for Mobile Ad-hoc Networks. Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'05), 551-557.

[3] Mauve, M., Widmer, J., Hartenstein, H. (2001). A Survey on Position-Based Routing in Mobile Ad-Hoc Networks. IEEE Network, 15(6), 30 – 39.

[4] Wu, X. (2005). VPDS: Virtual Home Region based Distributed Position Service in Mobile Ad Hoc Networks. Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICSCS 2005), 113-122.

[5] Takagi, H., Kleinrock, L. (1984). Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals. IEEE Transactions on Communications, 32(3), 246-257.

[6] Basagni, S., Chlamtac, I., Syrotiuk, V., Woodward, B. (1998). A distance routing effect algorithm for mobility (DREAM). Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), 76-84, Dallas, TX, USA.

[7] Ko, Y., Vaidya, N. (2000). Location-Aided Routing (LAR) in mobile ad hoc networks. Wireless Network (WINET), 6(4), 307-321, ACM.

[8] Liao, W., Tseng, Y., Sheu, J. (2001). GRID: A fully location-aware routing protocols for mobile ad hoc networks. Telecommunication Systems, 18, 61-84.

[9] Blazevic, L., Buttyan, L., Capkum, S., Giordano, S., Hubaux, J., Le Boudec, J. (2001). Self-organization in mobile d-hoc networks: the approach of terminodes. IEEE Communication Magazine, 39(6), 166-174.

[10] Zaruba, G., Chaluvadi, V., Suleman, A. (2003). LABAR: Location Area Based Ad Hoc Routing for GPS-Scarce Wide-Area Ad Hoc Networks. Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom'03), 509-513.

[11] Carter, S., Yasinsac, A. (2002). Secure Position Aided Ad Hoc Routing. Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02), 329-334, Cambridge.

[12] Mizanur Rahman, Sk., Mambo, M., Inomata, A., Okamoto, E. (2006). An Anonymous On-Demand Position-based Routing in Mobile Ad Hoc Networks. Proceedings of the International Symposium on Applications and the Internet, 300-306, Mesa/Phoenix, Arizona, USA, IEEE.

[13] Giordano, S., Stojmenovic, I., Blazevic, L. (2003). Position Based Routing Algorithms For Ad Hoc Networks: A Taxonomy. In Cheng, X., Huang, X., Du, D.Z. Ad hoc wireless Networking, (pp. 103-136), Kluwer. http://www.site.uottawa.ca/~ivan/routing-survey.pdf

Liana Khamis Qabajeh received her B.Sc. from Palestine Polytechnic University (PPU), Palestine in 2000 in Computer Engineering and joined the Engineering and Technology Faculty, PPU, as a research assistant. She received her M.Sc. from Jordan University of Science and Technology, Jordan in 2005 in Computer Engineering. Between 2005 and 2008 before pursuing her study, she was primarily involved in academic teaching and research in PPU. She is now working towards Ph.D. in Computer Science in University of Malaya, Malaysia. Her current research interests include Distributed Systems and Ad-Hoc Networks.

Dr. Miss Laiha Mat Kiah B.Sc. Comp. Sc. (Hons) (Malaya), M.Sc. (London) Ph.D. (London), joined the Faculty of Computer Science & Information Technology, University of Malaya, Malaysia as a tutor in 1997. She was appointed as a lecturer in 2001. She received her B.Sc. (Hons) in Computer Science from the University of Malaya in 1997, a M.Sc. from Royal Holloway, University of London UK in 1998 and a Ph.D. also from Royal Holloway, University of London in 2007. Between 1999 and 2003 before pursuing her study, she was primarily involved in academic teaching and research in University of Malaya. She was appointed as a senior lecturer in 2008 and currently she is the Head of Computer Systems and Technology Department. Her current research interests include key management, secure group communication and wireless mobile security. She is also interested in routing protocols and ad-hoc networks.

Mohammad M. Qabajeh received his B.Sc. from Palestine Polytechnic University, Palestine in 2000 and M.Sc. from Jordan University of Science and Technology, Jordan in 2006 in computer Engineering. He worked as a network administrator in one of the offices of the Palestinian government in the periods (2000-2003) and (2006-2008). During these periods he worked as a part time lecturer in many Palestinian universities. He is now working towards Ph.D. in Computer Engineering in International Islamic University Malaysia, Malaysia. His current research interests include Distributed Systems and Ad Hoc Networks.