Secure Unicast Position-based Routing Protocols for Ad-Hoc Networks

Liana Khamis Qabajeh, Miss Laiha Mat Kiah

Faculty of Computer Science and Information Technology
University of Malaya
58200 Kuala Lumpur, Malaysia
liana_tamimi@ppu.edu; misslaiha@um.edu.my

Mohammad Moustafa Qabajeh

Department of Electrical and Computer Engineering
International Islamic University Malaysia
58200 Kuala Lumpur, Malaysia
m_qabajeh@yahoo.com

Abstract: Ad-Hoc networks are decentralized wireless networks. A fundamental problem in Ad-Hoc networks is finding a secure and correct route between a source and a destination efficiently. The need for scalable and energy efficient routing protocols, along with the availability of small, inexpensive and low power positioning instruments, results in making position-based routing protocols a promising choice for mobile Ad-Hoc networks. This paper presents an extensive overview of the existing Ad-Hoc unicast routing protocols that make forwarding decisions based on the geographical position of the destination of a packet, while keeping security issues in mind. We outline the main problems for this class of routing protocols and a qualitative comparison of the existing protocols is done in regards to both security and performance issues. We conclude our work by investigating some future research opportunities.

Keywords: secure, unicast, position-based routing, location-aware routing, ad-hoc networks, wireless networks, routing protocols

1 Introduction

An Ad-Hoc network is considered as a very particular network since it is a self-organizing network with no pre-deployed infrastructure and no centralized control; instead, nodes carry out basic networking functions like routing. With this flexibility, Ad-Hoc networks have the ability to be formed anywhere and at any

time. In addition to traditional uses such as for military battlefields, these networks are being increasingly used in every-day applications, such as in conferences, personal area networking and meetings.

Routing protocol in Ad-Hoc networks is a fundamental part of the network infrastructure that supports the delivery of packets. It is a challenging task, as it has to face the challenge of link instability, frequently changing topology, the absence of a fixed infrastructure and low transmission power. Also, owing to differences in transmission capacity, some of the links may be unidirectional, which leads to the existence of asymmetric links.

All nodes in the network act as routers; hence security in routing protocols is necessary to guard against attacks, such as eavesdropping, spoofing, misdirection and the generating of deceptive routing messages. Moreover, wireless networks are generally more susceptible to physical security risks than wired networks. Therefore, routing in Ad-Hoc networks is a difficult task to accomplish efficiently, robustly and securely.

Several routing protocols have been proposed for Ad-Hoc networks. 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. However, position-based routing protocols use the nodes' geographical positions to make routing decisions, which improves performance and efficiency.

Although topology-based routing protocols (such as *DSR* [8] and *AODV* [7]) represent important steps in Ad-Hoc routing research area, some of these are not scalable and still exhibit security vulnerabilities. Even secure ones (such as *SAODV* [12], *ARIADNE* [37] and *ARAN* [22]) have some problems, such as single point of attack and failure, increased packet and processing overhead, as well as delays in the route discovery process. These problems become worse if these protocols are implemented in large networks since any request packet is flooded to the entire network.

Position-based Ad-Hoc routing protocols have proved to have better performance than traditional topology-based ones in end-to-end throughput and network scalability. Many position-based routing protocols have been proposed for Ad-Hoc networks such as *MFR* [16], *DIR* [11], *GPSR* [5], *ARP* [32], I-*PBBLR* [34] *DREAM* [28], *LAR* [38], *LARWB* [30], *LABAR* [13], *GRID* [33] and *TERMINODES* [23]. Although each of these protocols employs different techniques the basic goal is the same: only nodes making forward progress toward the destination are supposed to be involved in the route discovery process in an attempt to decrease the overall routing overhead.

These protocols require that a node be able to obtain its own, as well as the destination's geographical position. Generally, this information is obtained via Global Positioning System (GPS) and location services. The routing decision at

each node is then based on the destination's position contained in the packet and the position of the forwarding node's neighbors. So packets are delivered to the nodes in a particular geographic region in a natural way. There are different kinds of position-based protocols, which can be categorized into three main groups: *Restricted Directional Flooding (RDF), greedy* and *hierarchical* protocols [27] (to be discussed in Section 2).

All the aforementioned position-based routing protocols are exposed to some attacks as they focus on improving performance while disregarding security issues [31]. Recently some secure unicast position-based routing protocols have been proposed for mobile Ad-Hoc networks; *SPAAR* [29], *AODPR* [31] and *SGF* [21].

This survey is a continuation of our work in [24] and [26]. Our previous works have discussed position-based routing in general. In this paper, however, we have concentrated mainly on security issues by providing an extensive overview of the existing *secure* position-based routing protocols for Ad-Hoc networks. We outline the main problems that need to be solved for this class of routing protocols and present the solutions that are currently available. The discussed protocols are also compared with respect to the security level they achieve, the used location service, the used forwarding strategy, tolerability to position inaccuracy, robustness, implementation complexity, scalability, packet and processing overhead, guaranteeing loop-freedom, probability of finding the shortest path as well as the suitable network density for deployment.

The rest of the paper is organized as follows. Section 2 presents the basic idea and principles of position-based routing. Section 3 tackles security issues and requirements in Ad-Hoc networks routing protocols. Section 4 gives an overview of the selected secure position-based routing protocols. Sections 5 and 6 contain a qualitative comparison as well as analysis and discussion of the presented protocols. Future research directions are outlined in Section 7. Finally, we conclude the paper in Section 8.

2 Basic Principles of Position-based Routing

An important requirement of position-based routing is for the source node to be able to obtain the current position of the destination node. Usually a location service is responsible for this task. Existing location services are classified according to how many nodes host the service. This can be either some specific nodes or all nodes of the network. Additionally, each location server may maintain the position of some specific or all nodes in the network. The four possible combinations can be summarized as some-for-some, some-for-all, all-for-some and all-for-all [27].

Three main packet-forwarding strategies are used for position-based protocols: *greedy forwarding*, *Restricted Directional Flooding (RDF)* and *hierarchical* approaches. While their main objective is to utilize available position information in the Ad-Hoc routing, their means to achieve it are quite different. Most position-based protocols (such as *MFR*, *DIR*, *GPSR*, *ARP* and I-*PBBLR*) use *greedy forwarding* to route packets from a source to the destination. Greedy protocols do not establish and maintain paths between sources and their destinations; instead, a source node includes the position of the data packet's destination and selects the next hop depending on the optimization criteria of the algorithm, the nearest neighbor to the destination for example. Each intermediate node selects a next hop node until the packet reaches the destination. In order for the nodes to be able to do so, they periodically broadcast small packets (called beacons) to announce their position and enable other nodes to maintain a 1-hop neighbor table.

Some greedy position-based routing protocols, such as *MFR*, try to minimize the number of hops by selecting the node with the largest progress; i.e., the projection of the distance of the next hop from the sender on the straight line between the sender and the destination. Compass routing algorithms, such as *DIR*, try to minimize the spatial distance that a packet travels and base on forwarding the packet to the neighboring node that minimizes the angle between itself, the previous node and the destination. Whatever the used optimization criteria is, greedy forwarding is efficient, scalable and resilient to topology changes since it does not need routing discovery and maintenance. Greedy forwarding 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.

On the other hand, periodic beaconing creates lot of congestion in the network and consumes the nodes' energy [32]. While the beaconing frequency can be adapted to the degree of mobility, a fundamental problem of inaccurate (outdated) position information is always present; 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 increases the load on the network, creates lot of congestion, increases the probability of collision with data packets and consumes the nodes' energy [34].

Unfortunately, greedy routing may not always find the optimum route, and it may even fail to find a path between source and destination when one exists [21]. An example of this problem is shown in Fig. 1. The problem here is that *S* is closer to the destination *D* than any of the nodes in its transmission range; greedy forwarding will reach a local maximum even if there is a valid path from *S* to *D*. Generally, greedy forwarding works well in dense networks, but in sparse networks it fails due to voids; i.e., regions without nodes [11].

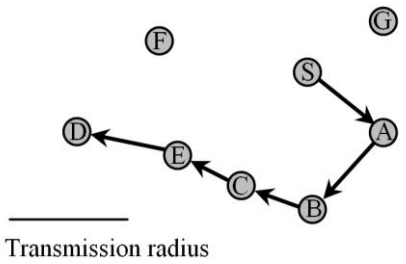

Figure 1
Greedy routing failure example

Finally, *DIR* and any other method that includes forwarding a message to a neighbor with closest direction are not loop-free as shown in [17] using the counterexample in Fig. 2. In DIR the source or intermediate node *A* uses the location information of the destination *D* to calculate its direction. Then the message m is forwarded to the neighbor *C*, such that the direction AC is closest to the direction AD. Referring to Fig. 2 the loop consists of four nodes denoted *S*, *B*, *C* and *A*. The transmission radius is as indicated in the figure. Let the source be any node in the loop, e.g. *S*. Node *S* selects node *B* to forward the message, because the direction of *B* is closer to destination *D* than the direction of its other neighbor *A*. Similarly node *B* selects *C*, node *C* selects *A*, and node *A* selects *S*.

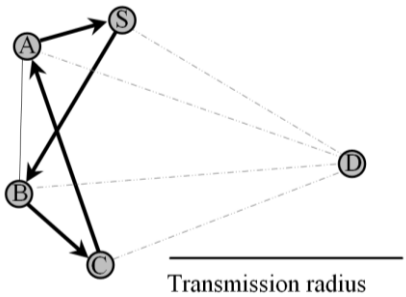

Figure 2
A loop in the directional routing

In *RDF*, such as *DREAM*, *LAR*, *LARWB* and *MLAR*, the sender will broadcast the packet to all 1-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 *RDF*, 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 the robustness against a failure of individual nodes and position inaccuracy. On the other hand, they have higher communication complexity than greedy ones and, therefore, have less scalability to large networks.

The last forwarding strategy is to form a *hierarchy* in order to scale to a large number of mobile nodes. Some strategies combine nodes' locations and hierarchical network structures by using zone based routing such as *LABAR*. Others use dominating set routing such as *GRID*. Some others, such as *TERMINODES*, 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; as a result, they inherit some characteristics of greedy forwarding.

We note that none of the above mentioned position-based routing protocols defined their security requirements and that they inherently trust all participants. Obviously, this could result in security vulnerabilities and exposures that could easily allow routing attacks. Recently, 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)* [29], *Anonymous On-Demand Position-based Routing in Mobile Ad-Hoc Networks (AODPR)* [31] and *Secure Geographic Forwarding (SGF)* [21]. These protocols are discussed in details in Section 4.

3 Security Issues in Ad-Hoc Routing Protocols

Ad-Hoc network security, in particular routing protocols security, has attracted more attention recently. Securing Ad-Hoc routing faces many challenges, especially that each user brings to the network his/her own mobile unit, without any centralized control such as is found in a traditional network. In Ad-Hoc routing protocols, nodes exchange information with each other about the network topology, constructing a virtual view of the network topology to allow the routing of the data packet. This information allows them to create, delete and update routes between the nodes of the network. On the other hand, this capability can pose a security weak point in Ad-Hoc networks because a compromised node could give bad information to redirect traffic or simply stop it. Thus, this information must be protected to avoid malicious nodes disrupting the network [15].

Securing Ad-Hoc routing faces difficulties which do not exist in wired networks, nor in infrastructure-based wireless networks. These difficulties make trust establishment among nodes virtually impossible [4]. Among these difficulties are the wireless medium itself and its physical vulnerability, the lack of centralized control and permanent trust infrastructure, the cooperation of nodes, restricted power and resources, highly dynamic topology and short-lived connectivity and availability, implicit trust relationship between neighbors and other problems associated with wireless communication [4] [15].

To ensure the security of Ad-Hoc networks, a number of requirements need to be satisfied. These requirements are availability, confidentiality, integrity, authentication and non-repudiation [2] [6] [25]:

- Availability: the network should remain operational and available to send and receive messages at any time. It is supposed to be robust enough to tolerate link failure and survive despite attacks.
- Confidentiality: provides secrecy to sensitive data being sent over the network; the contents of every message can be understood only by its source and destination. Although an intruder might get hold of the data being sent, he should not be able to derive any useful information.
- Integrity: ensures that messages being sent over the network are not corrupted by intentional or accidental modification.
- Authentication: ensures the identity of the nodes in the network, to assure that they are who they claim to be.
- Non-repudiation: guarantees that neither sender nor receiver can deny that he has sent or received the message.

Recently, as privacy has emerged as an important security issue, plenty of work on anonymous routing has been done (such as *ANODR* [18], *SDAR* [1], *ASRP* [35], *ODAR* [9] and *A3RP* [20]). Anonymity in an Ad-Hoc routing means that the identity of node, route path information, and location information should be veiled from not only an adversary, but also other valid nodes.

4 Secure Position-based Ad-Hoc Routing Protocols

In this section the selected protocols are described. For each protocol, we tried to summarize its main objectives, the basic security mechanisms used, how it works and its advantages and disadvantages compared to other protocols. Additionally, a performance analysis is conducted, taking into consideration the following evaluation criteria:

- Location service type: indicates the type of the location service used with the given protocol, i.e., shows how many nodes participate in providing location information and for how many other nodes each of these nodes maintains location information.
- Location service robustness: it is considered to be low, medium or high depending on whether the position of a given node will be inaccessible upon the failure of a single node, the failure of a small subset of the nodes or the failure of all nodes, respectively.

- Approach: describes the fundamental strategy used for packet forwarding.
- Tolerable position inaccuracy: forwarding strategies tolerate different degrees of inaccuracy of the position of the destination. This is reflected by the tolerable position inaccuracy criterion.
- Robustness: the robustness of a particular protocol is considered as 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 node might lead to the loss of the packet but does not require the set up of a new route. Finally, it is low if the failure of an individual node might result in packet loss and the setting up of a new route. Thus, the routing protocols that start data transmission immediately without 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 an increasing number of nodes in the network.
- Packet overhead: refers to bandwidth consumption due to larger packets and/or a 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 position-based routing protocols have lower packet overhead compared to other types, but this criterion is defined to compare the discussed protocols together.
- Processing overhead: is used to associate each protocol with the processing requirements. Low processing refers to approaches that require a low CPU processing.
- Loop-freedom: any routing protocol should be inherently loop-free to preserve the network resources and guarantee the correct operation of the protocol. Therefore, the discussed protocols are classified as having or not having loop-freedom property.
- Optimal path: is used to indicate the protocol probability of finding and using the shortest path for data packet relay.
- Density: indicates whether the protocol is more suitable to be implemented in dense or sparse networks.

4.1 SPAAR

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 environments 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. SPAAR provides the necessary requirements to secure routing in a high-risk environment: authentication, non-repudiation, confidentiality, and integrity. It uses asymmetric cryptography to protect against malicious nodes, which are unauthorized nodes that attempt to disrupt the network. Also it attempts to minimize the potential for damage of attacks from compromised nodes which are authorized nodes which have been overtaken by an adversary.

Two of the well-known attacks are the invisible node attack and the wormhole attack. In the invisible node attack, a malicious node may forward a packet without appending its address to the address field of that packet. The wormhole attack involves the cooperation between two malicious nodes sharing a private communication. One attacker captures routing packets at one point of the network and tunnels them to another point in the network. The new attacker then selectively injects tunneled traffic back into the network. SPAAR prevents both the invisible node attack and the wormhole attack by allowing the nodes to accept routing messages only from 1-hop neighbors.

To participate in SPAAR, each node requires a public/private key pair, a certificate binding its identity to its public key (signed by a Certificate Authority (CA) server), and the public key of that CA. Additionally, each node maintains two keys for each neighbor. The first is the neighbor's public key, which is obtained from its certificate and used to encrypt some routing messages such as Route REPly (RREP). The second is the neighbor's group decryption key, which is used to decrypt some routing messages such as Route REQuest (RREQ) to verify that the sender is a 1-hop neighbor.

Each node periodically broadcasts a "table update" message to inform the neighbors about its new position coordinates and transmission range. Each node maintains a neighbor table that contains the identity and position information of each verified neighbor, as well as the cryptographic keys required for secure communication with each neighbor; the used location service is all-for-some.

Additionally, each node maintains another table for the recent destinations it has communicated with. This table is similar to the neighbor table, except that the destination table also contains information about the speed of the node, making it possible to predict the node's next position. 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.

Route instantiation is triggered by the source through broadcasting a RREQ that is encrypted with its group encryption key. SPAAR uses a RREQ sequence number which is incremented each time a node initiates a RREQ and used to prevent replays of RREPs. RREQ recipients decrypt it with the appropriate group decryption key to verify that the sender of the RREQ is a 1-hop neighbor. The intermediate node checks if it or any of its neighbors is closer to destination; if so, it will encrypt the RREQ with its group encryption key, forward the RREQ and record the address of the predecessor neighbor; otherwise the RREQ is discarded. This process is repeated until the destination is reached. Upon receiving a RREQ, the destination constructs a 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.

Intermediate nodes, upon receiving a RREP, decrypt it with their private key and verify the signature with the public key of the neighbor node they received it from. Then they sign the RREP and encrypt it with the public key of the next node in the reverse route. Upon receiving the RREP, the successful decryption and the signature verification, the source begins sending data.

In SPAAR, each node maintains a neighbor table that contains the identity and position information of each verified neighbor; the used location service type is all-for-some. The source node can calculate the approximate geographic location of the destination from the most recent location and most recent velocity information stored in the source node's destination table. On the first attempt at communication with a particular destination, the source may use a location service or a selective flooding algorithm to reach the destination and receive its position information. The general robustness of this approach is medium, since the position of a node will become unavailable if a significant number of nodes fail.

SPAAR uses the *RDF*, so it exhibits properties such as the high probability of using the optimal path. Moreover it is loop free since it forwards packets to nodes towards the destination and uses a sequence number. SPAAR tolerates position inaccuracy by the expected region; each node forwards the RREQ only if it, or any of its neighbors, is closer to the destination. Its robustness is low since the failure of an individual node might result in packet loss and the setting up of a new route. SPAAR has high implementation complexity since messages must be verified, signed with the private key and encrypted with the public key of a neighbor. But it is still less complex than SGF since there is no reputation system.

SPAAR assumes the existence of one certificate server, which may be the operation bottleneck especially in large networks. Also, increasing the number of nodes in the network with using *RDF* will increase the packet overhead. Additionally, in large area networks the probability of having long routes is increased, and since each node spends time in signing and encrypting the messages, the probability of nodes movement and routes breakage are also increased. For these three reasons, SPAAR's scalability is considered as medium.

Moreover, SPAAR has a high packet overhead due to large-size packets resulting from the security techniques used along with the increased number of packets compared to greedy forwarding. These security techniques lead also to high processing overhead.

Finally, SPAAR can be implemented in both sparse and dense networks. It is suitable for sparse networks since it uses *RDF*, not greedy. Also, it is suitable for dense networks since increasing the number of neighbors will cause a larger neighbor table, but the computational overhead for the encryption of messages remains constant [29].

4.2 AODPR

Due to the dynamic, infrastructure-less and broadcast nature of MANETs, communications in these networks are susceptible to malicious traffic analysis. As a following step, an attacker may determine a target node and conduct an intensive attack against it, called a target-oriented attack. AODPR keeps routing nodes anonymous, thereby preventing possible traffic analysis. A time variant temporary identifier is computed from the time and position of a node in an attempt to keep the node anonymous. Moreover, it uses the concept of Virtual Home Regions (VHR), 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 Position Servers (PSs).

When a node joins the network, it registers to the PS and gets a Common Key (CK) and a public/private key pair from the PS. When a node wants to get position information of other nodes, it first sends a signed request and authenticates itself to the PS; accordingly the PS provides it with the required position information, the public key of the destination and other needed information. Then the source estimates the minimum Number of Hop (NH) which the route request packet travels to find a route from the source to the destination. Each intermediate node decrements NH by 1 and compares the updated NH with the minimum number of hop which the route request packet travels to find a route from this node to the destination (NH'). If NH' is less than or equal to NH, then the intermediate node forwards the packet to its neighbors and keeps the needed route information; otherwise it discards the packet. Both NH' 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.

To improve the security of their protocol, the position of the destination is encrypted with CK in the route request phase; hence there is no position information exposure to nodes outside the intended network. After authenticating the sources, the destination replies by a route reply and keeps the route information to itself. Upon receiving the route reply and authenticating the

destination, the source begins sending the data encrypted by the destination's public key. If source receives a fail packet, then it tries again with a new, larger estimated NH.

AODPR is robust against the wormhole attack in which an attacker records a packet in one location of the network and sends it to another location, making a tunnel; later it is retransmitted to the network under its control. Therefore, a packet might travel a long distance before finding the route from the source to the destination. In AODPR source nodes as well as intermediate nodes wait for a limited time to get a response. If the attacker response exceeds the limited time then it cannot be a forwarder within a routing path. So the effect of the wormhole attack is not effective in AODPR.

Although the AODPR is applicable to any node density in a network, ensures the anonymity of both route and nodes, and is robust against the target-oriented attack [31], it suffers from many problems. Many fields such as NH and destination position are encrypted using the CK; if this key is compromised, a large percentage of the communication in the whole network will be compromised. Moreover, AODPR suffers from two problems inherited from the VHR approach. First, nodes may be hashed to a VHR distant from the one they are currently residing in, leading to increased communication and time complexity, as well as to 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 VHR due to regions not including nodes.

In AODPR each PS keeps the position information of the nodes that hashed into its VHR; hence, the used location service type is some-for-some. Accordingly, a given node will be inaccessible upon the failure of the PSs of its VHR; i.e., its location service has medium robustness. AODPR uses the *RDF*, so its probability of using the optimal path is high. Moreover it is loop-free since it depends on forwarding the packets to the nodes towards the destination and uses a sequence number. AODPR tolerates to position inaccuracy by using the expected region. Its robustness is 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 and SGF since it does not use neighbor public key or reputation system.

AODPR has a medium scalability since increasing the number of nodes in the network with the usage of *RDF* 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 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. Finally, AODPR is applicable to any node density in a network [31]. It

is suitable for sparse networks, since it uses *RDF*, as well as dense networks, since increasing the number of nodes will cause larger position information tables in the PSs without affecting computational overhead for encrypting messages.

4.3 SGF

In [21] the SGF mechanism was proposed. It provides source authentication, neighbor authentication and message integrity by using both the shared key and the Instant Key disclosure (TIK) protocol [36]. By combining SGF with the Grid Location Service (GLS) [19], they proposed the Secure Grid Location Service (SGLS) where any receiver can verify the correctness of location messages. In this paper also a Local Reputation System (LRS) is proposed to detect and isolate compromised as well as selfish users.

The SGF mechanism incorporates both the hashed Message Authentication Code (MAC) [14] and the Timed Efficient Stream Loss-tolerant Authentication (TESLA) [3] with TIK protocol. The MAC is computed over the non-mutable part (e.g., the location information of a destination) of unicast messages with the pair-wise shared secret key between the source and destination.

Instead of introducing overhead by signing the destination's location information of all data and control messages, they proposed the use of a reputation system, LRS, to classify nodes as good or bad and to detect as well as isolate message tampering and dropping attackers. In LRS, each node only needs to manage the reputation information of its local neighbors and periodically send the reputation information report to its neighbors by using the HELLO messages. The TIK protocol with tight time synchronization is used to authenticate a previous forwarding node in order to prevent malicious users from joining a path and to avoid a message replay attack, re-sending recorded old valid control messages. Finally, when the destination receives a message, it can verify the authenticity of the message by comparing the received MAC to the MAC value that is computed over the received message with the secret key it shares with the source node.

In combination with SGF, the secure location service, SGLS, was proposed by combining SGF with the GLS so that any receiver can verify the correctness of location messages. The original GLS is a distributed location service in which each node maintains information about the locations of specific subsets of the nodes based on the node's identifiers. GLS divides the area that contains a MANET into a hierarchy of squares. Each node periodically broadcasts the list of neighbors it has. Consequently, each node can maintain a table of immediate neighbors as well as each neighbor's neighbors. Each node enlists nodes with IDs ''close'' to its own ID to serve as its Location Servers (LSs) by sending location update messages.

The general concept of the proposed SGF can generally be applied to any unicast message of GLS such as location query and location reply. So the 1-hop

neighbor's location information can be verified by using a location verification technique, and the TIK protocol can be used for neighbor authentication. The TESLA broadcast authentication method is used to verify the location information of 2-hop neighboring nodes. Unlike other messages, the location update message has no assigned destination address field in it. Thus, it is unfeasible to provide source authentication with a symmetric secret key. Hence, a public key infrastructure is assumed in the MANET under consideration. Each node stores the trusted CA's public key and signs the location update message with its private key.

The simulation results in [21] showed that SGLS can operate efficiently by using effective cryptographic mechanisms. Results also showed that LRS effectively detects and isolates message dropping attackers from the network. On the other hand, the simulations showed that the average end-to-end delay for SGLS is slightly higher than that of GLS, and that SGLS's routing overhead is significantly higher than that of GLS. This is obviously due to the increase in size of routing control messages with digital signatures and MACs in SGLS.

Generally, systems using a reputation system along with a cryptography scheme in order to defend against both compromised and malicious nodes do not scale well since they have to track the reputation of all nodes, which might require huge tables of information that are difficult to manage and to keep up to date [10]. Moreover, SGF assumes the existence of pair-wise shared secret keys between the nodes, which is difficult to implement in large area networks. Another drawback is that SGF assumes all nodes have tightly synchronized clocks, which is somewhat impractical for Ad-Hoc networks. Finally, it uses the greedy forwarding, which is not guaranteed to find the optimal path.

In SGF, each node should maintain a table of its immediate neighbors as well as each neighbor's neighbors [21]. So the used location service type is all-for-some. Accordingly, a given node will be inaccessible upon the failure of a subset of the nodes; the robustness of its location service is medium. SGF uses the greedy forwarding, so it exhibits some greedy properties such as uncertainty of using the optimal path. SGF 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.

SGF tolerates to position inaccuracy by the list of neighbors HELLO messages that each node periodically broadcasts; each node knows the exact position of nodes in its transmission range and neighbors' transmission ranges.

It is clear that it is very complex to implement SGF since it uses many securing techniques whether with the location service or the forwarding strategy. SGF assumes the existence of pair-wise shared secret keys between the nodes, which is difficult to implement in large area networks; so it has medium scalability. Moreover it has a high packet overhead due to the periodically sent reputation information report and the list of neighbors HELLO messages, in addition to the

large-size packets due to the security techniques used. These security techniques lead also to high processing overhead. SGF loop freedom depends on the used optimization criteria (directional or other). Finally, SGF is preferably implemented in moderate density networks, since greedy forwarding may have problems in sparse networks. On the other hand, implementing it in a dense network will increase the size of the periodic list of neighbors and reputation information HELLO messages, which may consume the network bandwidth and the nodes' memory.

5 Comparison of Discussed Protocols

Table 1 summarizes the discussed secure position-based protocols together with the security and performance evaluation criteria used. The three discussed protocols utilize position-based routing to achieve better performance than other topology-based ones while considering security issues and requirements.

SPAAR provides the necessary requirements to secure routing in hostile environments by assuring authentication, non-repudiation, confidentiality and integrity. It uses asymmetric cryptography to protect against malicious and compromised nodes. SPAAR uses the *RDF* resulting in high probability of using optimal paths. Furthermore SPAAR is loop free due to forwarding packets to nodes towards the destination and using sequence numbers. It tolerates to position inaccuracy via the expected region; i.e., each node forwards the RREQ only if it or any of its neighbors is closer to the destination. Its robustness is considered as low since the failure of an individual node might result in packet loss and the setting up of a new route. The implementation complexity of SPAAR is high since messages must be verified, signed with the private key and encrypted with the public key of a neighbor.

SPAAR is considered to have a medium scalability due to three reasons. SPAAR assumes the existence of a certificate server resulting in a system operation bottleneck, especially in large area networks. Moreover, increasing number of nodes, along with the use of *RDF*, results in high packet overhead. Finally, in large area networks, the probability of having long routes is high, and since each node spends time signing and encrypting routing messages, the probability of node movement and route breakage is increased. SPAAR has a high packet overhead due to large-size packets resulting from the security techniques used and an increased packets number compared to greedy forwarding. These security techniques result also in increased processing overhead. Lastly, SPAAR is suitable for implementing in both sparse and dense networks. It is suitable for sparse networks due to the usage of RDF. It is also suitable for dense networks since the increased number of neighbors causes a larger neighbor table but does not affect the computational overhead for message encryption.

Table 1
Characteristics of the presented secured position-based routing protocols

Criterion	SPAAR [29]	AODPR [31]	SGF [21]
Security mechanism	Certificates and timestamps	Symmetric and asymmetric cryptography and hash functions	Symmetric and asymmetric cryptography and hashed MAC algorithm
Synchronization	No	Yes	Yes
Central trust	Certificate Authority	Key Distribution Center	Certificate Authority
Main idea/ contribution	Uses cryptographic certificates to protect routing packets in managed-hostile environments	Keeps routing nodes anonymous to prevent possible traffic analysis and target-oriented attack	Provides source authentication, neighbor authentication and message integrity
Proposal	• Intermediate node checks if it or any of its neighbors is closer to destination it encrypts RREQ with its group encryption key so that recipients can decrypt it with the appropriate group decryption key and verify that the sender is a 1-hop neighbor. • Intermediate nodes sign the RREP with its private key and encrypt it with the public key of the neighbor it received the RREQ from and verify the signature with the public key of the neighbor node it received the RREP from.	• Uses VHRs; nodes' positions are reported to PSs. • Each intermediate node decides to broadcast the route request packet or not depending on the distance from the node to the destination and the radius of the maximum radio range coverage of each node. • Destination's position is encrypting with CK on the route request phase. • After authenticating the sources, the destination replies by a route reply. • Upon authenticating the route reply sender, source begins sending data encrypted by destination's public key.	• Uses a reputation system to detect and isolate message tampering and dropping attackers as well as a secure location service to verify the correctness of location messages. • The MAC is computed over the destination's location with the pair-wise shared secret key between source and destination to enable the destination to verify authenticity of message. • The TIK protocol is used to authenticate the predecessor and TESLA is used to verify the location information of 2-hop neighboring nodes.
Location service type	All-for-Some	Some-for-Some	All-for-Some
Location service robustness	Medium	Medium	Medium
Approach	Restricted directional flooding	Restricted directional flooding	Greedy

AODPR uses the *RDF*, resulting in a high probability of using the optimal path. Moreover, it is guaranteed to be loop-free since it depends on forwarding the packets to the nodes towards the destination and uses sequence numbers. AODPR tolerates to position inaccuracy by using the expected region. AODPR is robust against the wormhole attack and target-oriented attack. It is applicable to any node density and ensures routes and nodes anonymity. On the other hand, it suffers from numerous problems. For example, a large percentage of communication is done using the CK; hence it is a big concern to keep this key uncompromised.

AODPR's robustness is low since the failure of an individual node might result in packet loss and setting up a new route. In AODPR, messages are signed only with the private key of each node. Accordingly, its implementation complexity is less than SPAAR and SGF since it does not use neighbor public keys or a reputation system. AODPR has a medium scalability since increasing the number of nodes in the network with the usage of *RDF* increases the packet overhead. 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.

SGF provides source authentication, neighbor authentication and message integrity by using both the shared key and the Instant Key disclosure. SGF tolerates to position inaccuracy by the list of neighbors HELLO messages that each node periodically broadcasts; hence each node knows the exact position of nodes in its transmission range and its neighbors' transmission ranges.

It is clear that it is complex to implement SGF since it uses many securing techniques whether during the location service or the forwarding process. SGF assumes the existence of pair-wise shared secret keys among nodes, which is difficult to implement in large area networks; i.e., it has medium scalability. Moreover, it has high packet overhead due to the reputation reports and list of neighbors HELLO messages that are sent periodically, as well as to large-size packets due to the security techniques used. These security techniques result also in high processing overhead. SGF loop freedom depends on the used optimization criteria (directional or other). Finally, it is preferable to implement SGF in moderate density networks since greedy forwarding may have problems in sparse networks. On the other hand, implementing it in a dense network increases the size of the periodic list of neighbors and reputation information messages, which may consume the network's bandwidth and the nodes' memory.

Table 1
Characteristics of the presented secured position-based routing protocols (Continued)

Criterion	SPAAR [29]	AODPR [31]	SGF [21]
Tolerable position inaccuracy	Expected Region	Expected Region	Transmission range and neighbors' transmission range
Robustness	Low	Low	Medium
Implementation complexity	High	Medium	High
Scalability	Medium	Medium	Medium
Packet overhead	High	Medium	High
Processing overhead	High	Medium	High
Loop freedom	Yes	Yes	Depends on optimization criteria
Optimal path	High	High	Medium

Density	Both	Both	Moderate
Advantages	• Provides authentication, confidentiality, integrity and non-repudiation. • Provides high security level against malicious and compromised nodes as well as being robust against invisible node and wormhole attacks	• Provides authentication, confidentiality and Anonymity. • Ensures the anonymity of both route and nodes and robust against the target-oriented and wormhole attacks	• Provides authentication and integrity. • Effectively detects and isolates message dropping attackers from the network and robust against the replay attack
Disadvantages	• 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	• Suffers serious security problem if the CK is compromised. • Nodes may be hashed to a distant VHR leading to increased communication and time complexity and unreachable VHRs.	• Has scalability problem due to assuming pair-wise shared secret keys, assuming tightly synchronized nodes' clocks and tracking reputation of all nodes

6 Analysis and Discussion

The three presented protocols depend on position-based routing to achieve better performance compared to traditional topology-based ones while taking security issues into consideration. They aim to provide the necessary requirements to secure routing; however, they suffer from some problems limiting their scalability. SPAAR, for example, requires high processing time, since it uses asymmetric cryptography, not only for end to end communication, but also for hop-to-hop communications. SPAAR also has a centralized trust and so suffers from the compromised server problem and the single point of failure.

AODPR uses a common key; if this key is compromised a large percentage of the communication in the whole network will be compromised. Moreover, it suffers from increased communication and time complexity if the nodes are hashed to a distant VHR, as well as if the VHR of a node cannot be reached. Additionally, due to nodes' movement, it might be difficult to guarantee that at least one position server will be present in a given Ad-Hoc network. SGF on the other hand suffers from high average end-to-end delay and packet overhead. Moreover, SGF assumes the existence of pair-wise shared secret keys between the nodes, which is difficult to implement in large area networks. Another drawback is that SGF assumes all nodes have tightly synchronized clocks, which is somewhat impractical for Ad-Hoc networks. Finally, it uses the greedy forwarding, which is not guaranteed to find the optimal path.

As a summary, even though the three discussed protocols try to improve performance and security, they suffer from several problems, such as single point

of failure and attack, along with high packet and processing overhead as in SPAAR and SGF; and sharing single key among all nodes as in AODPR, as well as assuming pair-wise shared secret keys and tightly synchronized nodes' clocks as in SGF. Consequently, these problems result in limiting the scalability of the discussed protocols.

7 Directions of Future Research

This paper has demonstrated that there are many approaches to be considered for position-based packet forwarding. Even so, there still exist a number of issues that need to be addressed. Position-based protocols make it possible to have larger networks without scalability problems. However, geographical routing also introduces new opportunities for attackers, especially given that most protocols broadcast position information in a clear form, which allows anyone within range to receive it. Hence, node position can be altered, making other nodes believe that it is in a different position. This could make other nodes believe that the attacker is the closest node to the destination and choose it as the best candidate for the next hop.

Consequently, the attacker might be able to alter or drop the received packets. Thus, it is imperative that more intensive works be done for secure position-based routing protocols 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 needs to be addressed, since location privacy is hard to achieve when a node identifier can be immediately associated with its position.

Alternative security schemes that are not based on infrastructure for key distribution should be considered, especially given that they suffer from high processing requirement (due to signing and signature verification of every packet) and may be a perfect target for Denial of Service (DoS), where attackers try to exhaust a node's processing time and battery through forcing them to spend time doing cryptographic calculations that are not required. Moreover, approaches that suggest the usage of symmetric cryptography suffer from a scalability problem since every pair of nodes would require a unique shared key.

Geographical routing protocols depend heavily on the existence of secure 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 security and scalability points upon developing a new location service. Finally, the most common way to enable nodes to know 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.

Summary and Conclusions

Efficient routing protocol is one of the most important issues in mobile Ad-Hoc wireless networks. Many points should be considered when developing a routing protocol, such as a high delivery rate, a short path, a small flooding ratio, a small end-to-end delay, low power consumption, a high level of security and avoiding single point of failure. This study has presented the current state of secure position-based Ad-Hoc routing and provided a qualitative evaluation of the presented approaches. Lastly, we identified a number of research opportunities which could lead to further improvements in this field.

Position-based routing protocols use the geographical position of nodes to make routing decisions, which results in improving efficiency and performance. 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. 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 or it may not find a path at all. In *RDF* packets are broadcasted in the general direction of the destination. It was found that RDF protocols have better performance than greedy ones in term of finding the shortest path. Using *hierarchical* approaches increases the scalability of a routing protocol. 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.

Recently, security has gained attention in topology-based routing protocols and many attempts at proposing end-to-end security schemes have been made. However, it is clear that few research efforts have addressed position-based security issues. Even secure ones suffer from many problems. Some of these problems are single point of failure and attack, along with some problems regarding packet and processing overhead, as in SPAAR and SGF, sharing single key among all nodes as in AODPR as well as assuming pair-wise shared secret keys and tightly synchronized nodes' clocks as in SGF. Consequently, these problems result in limiting the scalability of the discussed protocols.

Without online trusted servers, it is difficult to be aware of the trustworthiness of each node, thus to exclude malicious nodes from the routes. Furthermore, the approach in which one centralized server is used in the Ad-Hoc network is not practical as the server may be mobile, and result in operation bottlenecks as well as system single point of failure and attack. In order to address this problem, the position service system and the certificate authority should be distributed among multiple servers. Hence, it is an important issue to develop a scalable, distributed, secure and position-based routing protocol for Ad-Hoc networks.

Acknowledgement

We want to thank the editors and the anonymous reviewers for their valuable effort and time. This work was done under the VotF University Malaya fund no. FS132/2008C and PPP University Malaya funds no. PS091/2009A and PS410/2010B.

References

[1] A. Boukerche, K. El-Khatib, L. Xu, L. Korba: SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks, in Proceedings of International Conference on Local Computer Networks (LCN '04), 2004, pp. 618-624

[2] A. Mahmoud: Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed-ARAN), Master thesis, Computer Science Department, The American University in Cairo, 2005 http://www.mbifoundation.com/media/18949/Abdalla%20Mahmoud%20-%20Thesis%20Defense.pdf

[3] A. Perrig, R. Canetti, D. Song, D. Tygar, B. Briscoe: TESLA: Multicast Source Authentication Transform Introduction, Internet Engineering Task Force, Internet Draft of Multicast Security Working Group, 2004 http://tools.ietf.org/html/draft-ietf-msec-tesla-intro-04.txt

[4] A. Pirzada, C. McDonald: Reliable Routing in Ad Hoc Networks Using Direct Trust Mechanisms. In M. Cheng, D. Li: Advances in Wireless Ad Hoc and Sensor Networks, 2008, pp. 133-159

[5] B. Karp, H. Kung: GPSR: Greedy Perimeter Stateless Routing for Wireless Networks, in Proceedings of 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 2000), Boston, Massachusetts, USA, 2000, pp. 243-254

[6] C. Murthy, B. Manoj: Ad Hoc Wireless Networks: Architectures and Protocols, ISBN:013147023X, Prentice Hall Communications Engineering and Emerging Technologies Series, Upper Saddle River, NJ, USA, 2004, pp. 213-214 & 475-490

[7] C. Perkins, E. Royer: Ad Hoc On-Demand Distance Vector Routing, in Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, 1999, pp. 90-100

[8] D. Johnson, D. Maltz: Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, Vol. 353, Kluwer Academic Publishers, 1996, pp. 153-181

[9] D. Sy, R. Chen, L. Bao: ODAR: On-Demand Anonymous Routing in Ad Hoc Networks, in Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Oct, 2006, pp. 267-276

[10] E. Fonseca, A. Festag: A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS, NEC Technical Report NLE-PR-2006-19, NEC Network Laboratories, 2006 http://www.network-on-wheels.de

[11] E. Kranakis, H. Singh, J. Urrutia: Compass Routing on Geometric Networks, in Proceedings of 11th Canadian Conference on Computational Geometry, Vancouver, 1999, pp. 51-54

[12] G. Zapata: Secure Ad hoc On-Demand Distance Vector Routing, ACM Mobile Computing and Communications Review, Vol. 6, No. 3, 2002, pp. 106-107

[13] G. Zaruba, V. Chaluvadi, A. Suleman: LABAR: Location Area-based Ad Hoc Routing for GPS-Scarce Wide-Area Ad Hoc Networks, in Proceedings of 1st IEEE International Conference on Pervasive Computing and Communications (PerCom'03), 2003, pp. 509-513

[14] H. Krawczyk, M. Bellare, R. Canetti: HMAC: Keyedhashing for Message Authentication, Internet Engineering Task Force, Request for Comment RFC 2104, 1997 http://www.ietf.org/rfc/rfc2104.txt

[15] H. Rifa-Pous, J. Herrera-Joancomarti: Secure Dynamic MANET On-demand (SEDYMO) Routing Protocol, in Proceedings of 5th Annual Conference on Communication Networks and Services Research(CNSR '07), Fredericton, NB, Canada, 2007, pp. 372-380

[16] H. Takagi, L. Kleinrock: Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals, IEEE Transactions on Communications, Vol. 32, No. 3, 1984, pp. 246-257

[17] I. Stojmenovic, X. Lin: Loop-Free Hybrid Single-Path/Flooding Routing Algorithms with Guaranteed Delivery for Wireless Networks, IEEE Transactions on Parallel and Distributed Systems, Vol. 12, No. 10, 2001, pp. 1023-1032

[18] J. Kong, X. Hong: ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks, in Proceedings of MOBIHOC '03, June 1-3, Annapolis, Maryland, USA, 2003, pp. 291-302

[19] J. Li, J. Jannotti, D. De Couto, D. Karger, R. Morris: A Scalable Location Service for Geographic Ad Hoc Routing, in Proceedings of 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 2000), Boston, Massachusetts, USA, 2000, pp. 120-130

[20] J. Paik, B. Kim, D. Lee: A3RP: Anonymous and Authenticated Ad Hoc Routing Protocol, in Proceedings of International Conference on Information Security and Assurance, 2008, pp. 67-72

[21] J. Song, V. Wong, V. Leung: Secure Position-based Routing Protocol for Mobile Ad Hoc Networks, Elsevier Ad Hoc Networks Journal, Elsevier, Vol. 5, 2007, pp. 76-86

[22] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, E. Belding-Royer: Authenticated Routing for Ad Hoc Networks, IEEE Journal on Selected Areas in Communications, Vol. 23, 2005, pp. 598-610

[23] L. Blazevic, L. Buttyan, S. Capkum, S. Giordano, J. Hubaux, J. Le Boudec: Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes, IEEE Communication Magazine, Vol. 39, No. 6, 2001, pp. 166-174

[24] L. Qabajeh, M. L. Mat Kiah, M. Qabajeh: A Qualitative Comparison of Position-based Routing Protocols for Ad-Hoc Networks, International Journal of Computer Science and Network, Vol. 9, No. 2, 2009, pp.131-140

[25] L. Zhou, Z. Haas: Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, Vol. 13, 1999, pp. 24-30

[26] M. L. Mat Kiah, L. Qabajeh, M. Qabajeh: Unicast Position-based Routing Protocols for Ad-Hoc Networks, Acta Polytechnica Hungarica, Vol. 7, No. 5, 2010, pp. 19-46

[27] M. Mauve, J. Widmer, H. Hartenstein: A Survey on Position-based Routing in Mobile Ad-Hoc Networks, IEEE Network, Vol. 15, No. 6, 2001, pp. 30-39

[28] S. Basagni, I. Chlamtac, V. Syrotiuk, B. Woodward: A Distance Routing Effect Algorithm for Mobility (DREAM), in Proceedings of 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), Dallas, TX, USA, 1998, pp. 76-84

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

[30] S. Kalhor, M. Anisi, A. Haghighat: A New Position-based Routing Protocol for Reducing the Number of Exchanged Route Request Messages in Mobile Ad-hoc Networks, in Proceedings of 2nd International Conference on Systems and Networks Communications (ICSNC 2007), 2007, p. 13

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

[32] V. Giruka, M. Singhal: Angular Routing Protocol for Mobile Ad-hoc Networks, in Proceedings of 25th IEEE International Conference on Distributed Computing Systems Workshops, 2005, pp. 551-557

[33] W. Liao, Y. Tseng, J. Sheu: GRID: A Fully Location-Aware Routing Protocols for Mobile Ad Hoc Networks, Telecommunication Systems, Vol. 18, 2001, pp. 61-84

[34] Y. Cao, S. Xie: A Position-based Beaconless Routing Algorithm for Mobile Ad Hoc Networks, in Proceedings of International Conference on Communications, Circuits and Systems, Vol. 1, IEEE, 2005, pp. 303-307

[35] Y. Cheng, D. Agrawal: Distributed Anonymous Secure Routing Protocol in Wireless Mobile Ad Hoc Networks, OPNETWORK, Aug. 2005, pp. 22-26

[36] Y. Hu, A. Perrig, D. Johnson: Packet Leashes: a Defense against Wormhole Attacks in Wireless Network, in Proceedings of 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, CA, Vol. 3, 2003, pp. 1976-1986

[37] Y. Hu, A. Perrig, D. Johnson: ARIADNE: A Secure On-Demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM'02), Atlanta, Georgia, USA, 2002, pp. 12-23

[38] Y. Ko, N. Vaidya: Location-aided Routing (LAR) in Mobile Ad Hoc Networks, Wireless Network (WINET), Vol. 6, No. 4, ACM, 2000, pp. 307-321