DETAILED PERFORMANCE EVALUATION OF ARANZ, ARAN AND AODV PROTOCOLS

[1]LIANA K. QABAJEH, [2]MOHAMMAD M. QABAJEH

[1]Faculty of Information Technology and Computer Engineering, Palestine Polytechnic University, Palestine

[2]Faculty of Engineering and Technology, Palestine Technical University Kadoorie, Palestine

E-mail: [1]liana_tamimi@ppu.edu, [2]mohammad.qabajeh@ptuk.edu.ps

ABSTRACT

Ad-Hoc networks are spontaneously formed when devices connect and communicate with each other. One of the significant issues in mobile Ad-Hoc networks is seeking an efficient and secure route from a specific source leading to an anticipated destination. In managed-open environments there is a chance for pre-deployment of some keys and certificates. ARANz protocol has been proposed to be implemented in such environments and utilized the authentication techniques of the original Authenticated Routing for Ad-Hoc Networks (ARAN). ARANz seeks to enhance security, attain robustness and solve single point of attack and failure problems by electing numerous certificate authority servers. Furthermore, ARANz ensures improved scalability and performance through dividing the network into zones and using restricted directional flooding.

A detailed and extensive simulated performance evaluation has been conducted to assess ARANz and compare it with ARAN protocol and Ad-Hoc On-demand Distance Vector (AODV). Results demonstrate that ARANz is able to discover secure routes effectively within relatively large networks having large number of mobile nodes, while attaining the minimum packet routing load. Results also show that ARANz has superior performance regardless nodes density, local communications percentage, zone size and failed nodes percentage.

Keywords: *Position-Based, Secure, Scalable, Routing Protocol, Mobile, Ad-Hoc Networks, Managed-Open Environment, Location Service, Performance Evaluation, Aranz, ARAN And AODV.*

1. INTRODUCTION

An Ad-Hoc network is a self-organizing multi-hop wireless network. Efficient routing is a key issue in Ad-Hoc networks since each node in the network acts as both a host and a router. Furthermore, the structure of Ad-Hoc networks result in making them prone to some attacks such as modification, fabrication and impersonation.

Managed-open environment may be found among students on a campus or peers at a conference. In this type of environments it is possible to use previously established infrastructure; i.e., there is a chance for pre-deployment of some keys and certificates. Nevertheless, depending on one centralized server is unfeasible for Ad-Hoc networks since it may be the operation bottleneck. In order to deal with this problem, the certificate authority and position service system should be distributed among numerous servers. The need for energy-efficient and scalable protocols, along with the recent availability of inexpensive and low-power positioning instruments, justify adopting position-based routing in mobile Ad-Hoc networks.

Hence, it is a need for scalable and secure position-based routing protocols for Ad-Hoc networks. Our work in [1] proposed a new hierarchal and distributed routing protocol, ARANz. Based on the original Authenticated Routing for Ad-Hoc Networks (ARAN) [2], ARANz seeks to achieve improved performance and distribute routing load by dividing the area into zones. Moreover, it looks for increasing robustness and security, as well as solving the single point of failure and attack problems by distributing trust among numerous certificate authority servers. Finally, ARANz aims to exhibit better scalability and robustness against common topological changes through using restricted directional flooding.

This paper is an extension of our work in [1]. A detailed discussion of the ARANz protocol, security analysis of both ARAN and ARANz protocols, as well as simplified simulated network performance evaluation among Ad-Hoc On-demand Distance Vector (AODV) [3], ARAN and ARANz protocols have been presented in [1]. Simulations in [1], however, have considered only nodes mobility and network size. This paper, on the other hand, presents a detailed simulated network performance evaluation and comparison among AODV, ARAN and ARANz protocols, taking into consideration the effect of node density, local communication, zone size, and node failure.

From the results, we found that ARANz is able to discover secure routes effectively regardless network size, nodes mobility, nodes density, local communications percentage, and zone size. Additionally, ARANz is still able to have superior performance even with having large percentage of malfunctioning (failed) nodes. Moreover, ARANz has achieved the scalability issue by maintaining the minimum packet routing load in all presented scenarios compared to AODV and ARAN protocols. The cost of ARANz is higher latency in route discovery on account of the time required for authentication and packet processing as well as obtaining destination position.

The paper is organized as follows. Section 2 introduces the existing and recent works on Ad-Hoc routing protocols. Section 3 presents ARANz protocol. Section 4 involves a simulated comparison among AODV, ARAN and ARANz protocols. Section 5 discusses our findings, and our work is concluded in Section 6. Finally, future directions are discussed in Section 7.

2. BACKGROUND

Ad-Hoc networks routing protocols can be categorized into two main types: topology-based and position-based. Topology-based routing protocols utilize network links information to make packet forwarding. They are, consequently, divided into three groups: proactive, reactive and hybrid protocols. Proactive routing protocols periodically transmit control messages in a try to make each node always knows a current route to other destinations. Proactive routing protocols are less appropriate for Ad-Hoc wireless networks since they constantly consume nodes power and they are not designed to track topology changes occurring at a high rate [4][5]. In contrast, reactive routing protocols are considered more fitting for wireless environments since they conduct a route discovery process only when having data to be sent to a particular destination. One advantage of reactive routing protocols, such as AODV, is that there is no need for periodic routing packets. Though, they may have high control overhead in high mobility networks and heavy traffic loads. Also, they have a scalability problem due to blind broadcast of route discovery packets [5]. Zone Routing Protocol (ZRP) [4] is an example of Hybrid routing protocols that try to combine the best properties of both proactive and reactive techniques. The drawback of ZRP is that for large zones the protocol acts like a proactive protocol, while for small zones it may act like a pure reactive protocol [6].

Generally, topology-based protocols cannot scale well for networks with more than several hundreds of nodes [7]. Additionally, none of Ad-Hoc routing protocols mentioned above defines their security requirements and they trust all participants. Apparently, this may result in security vulnerabilities and exposures that could easily allow routing attacks [2][8][9]. After that many secure routing protocols have been proposed such as [2][10][11][12][13][14][15]. One important protocol is the ARAN protocol, which is similar to AODV but affords authentication of route discovery, setup and maintenance in addition to message integrity and non-repudiation. ARAN assumes the existence of a trusted Certificate Authority (CA) server. In comparison to basic AODV, ARAN prevents a number of exploits such as modification, impersonation and fabrication. In contrast, ARAN causes more packet overhead and higher route discovery latency since each packet must be signed. As well, it has problems dealing with scalability issue regarding nodes number. ARAN also based on a centralized trust, therefore, suffers from the compromised server and single point of failure problems.

In recent developments, position-based routing protocols reveal better performance, scalability and robustness against continuous topological changes [7][16]. Position-based protocols use nodes geographical positions to make routing decisions, which results in improved efficiency and performance. Hence, nods should obtain their own geographical positions via Global Positioning System (GPS) and destination position by means of a location service. There are different categories of position-based routing protocols that includes: Greedy, Restricted directional flooding and hierarchical routing protocols.

In greedy forwarding, such as Greedy Perimeter Stateless Routing (GPSR) [17], each intermediate node selects its closest neighboring node to the destination as the next hop. Thus, each node periodically broadcasts small beacons to inform its neighbors about its position. Periodic beacons consume nodes energy and network bandwidth [7].

Also, greedy forwarding may not always discover the best route especially in sparse networks [17][18]. In restricted directional flooding, such as Location-Aided Routing (LAR) [19], source broadcasts the packet to all single hop neighbors towards the destination. When a route request message is received, the receiving node retransmits the message only if it is closer to the destination compared to its previous hop; otherwise, the message is dropped. One example of hierarchical routing protocols is TERMINODES [20], in which packets are routed based on a proactive distance vector if the destination is close to the sender and using greedy forwarding in long distance routing.

All the aforementioned position-based protocols are susceptible to various security attacks since they do not take into consideration the security issue [9]. Recently, a few Ad-Hoc secure position-based protocols have been suggested [21]. Some of them are an anonymous location-based efficient routing protocol in MANETs (ALERT) [22], Anonymous On-Demand Position-based Routing in Mobile Ad-Hoc Networks (AODPR) [9] and Secure Geographic Forwarding (SGF) [23]. However they still experience some dilemmas such as single point of failure and attack, high packet and processing overhead and/or scalability problems.

To conclude, we found that many topology-based routing protocols still have security weaknesses and are considered unscalable. Although some improvements on security aspects were proposed such as in ARAN, the implicit trust on a centralized node introduces other security problems. Like the others, ARAN does not scale well. Additionally, restricted directional flooding has better performance compared to topology-based and other position-based routing protocols.

3. PROPOSED PROTOCOL

In this section, ARANz routing model is represented. ARANz adopts the authentication steps used with the ARAN protocol and deals with the network as zones. ARANz, like ARAN, uses cryptographic certificates to prevent most of the attacks against Ad-Hoc routing protocols. However, ARANz introduces a hierarchal routing approach, to achieve better performance of the routing protocol and distribute load by dividing the network area into zones. Moreover, ARANz tries to achieve robustness, increase security, solve the single point of failure problem and avoid the single point of attack problem by distributing trust among multiple Local Certificate Authority (LCA) servers. Each zone contains multiple LCAs that should team up with each other to provide certificates to the local nodes. ARANz has also a Misbehaviour detection scheme to improve its security. Furthermore, ARANz tries to demonstrate better scalability and performance by adopting the restricted directional flooding. Consequently LCAs work also as position servers and nodes should inform LCAs of their zones about their new position if they moved.

ARANz consists primarily of five phases; network setup, network maintenance, location service, route instantiation and maintenance and finally data transmission. Network setup phase takes into account certifying trusted nodes, dividing area into multiple zones and deciding on initial certificate authority servers. Network maintenance phase deals with ensuring maintenance of the network structure considering some issues like updating nodes certificates, nodes movement, and corrupted and destroyed nodes. Whenever a node has data to be sent to a particular destination; it is supposed to obtain the destination position before conducting the route discovery process. Location service phase enables the source to obtain the destination position through communicating LCAs in its zone. After getting the destination position, route instantiation and maintenance phase is initiated by sending a route discovery packet using restricted directional flooding. After route discovery and setup, data transmission phase is initiated by the source via sending the data to the intended destination.

Nn cooperative nodes are assumed. They are distributed randomly in a square-shape area and are aware of their positions. A specific node is selected prior to the network deployment and has the required software to initiate the network setup, divide the area into zones and elect the initial LCAs. This node is called the Primary Certificate Authority (PCA) server and possesses the private part of the network key (K_{NET-}). All the trusted nodes participating in the network have a private/public key pair, the public part of the network key (K_{NET+}) and a Common Key (CK) which is used for encryption and decryption of the packets sent by all non-PCA nodes in the network setup phase.

Before proceeding further, let us define the following variables, notations and packet identifiers that are used in the upcoming sections. Table 1 summarizes the used packet identifiers.

Table 1 Packet identifiers for ARANz

3.1 Network setup

As a necessary step, the network setup phase starts with primary communications between PCA and other authorized non-PCA nodes. Through these communications, PCA collects information about other nodes to help it in certifying authorized nodes, dividing the area into zones, electing LCAs for each zone and informing nodes about their initial roles (LCA or regular node). In Table 2, the packets exchanged during the network setup phase of ARANz are summarized. Figure 1 shows network structure, if we suppose that the entire area is divided, for example, into sixteen zones.

Table 2: Packets sent during the network setup phase of ARANz

Figure 1: Network structure after electing initial LCAs

3.2 Network maintenance

During the network lifetime nodes may update their certificates, move freely in the network, move in and out the network and become corrupted. Table 3 summarizes packets sent to deal with these issues.

Table 3: Packets sent during the network maintenance phase of ARANz

3.3 Location service

The location service is used to enable the source node to obtain the position of a particular destination. Two cases are considered, local communications, i.e., the source and destination are in the same zone, and external communications, i.e., the source and destination reside in different zones. Before initiating route discovery, the source is supposed to get the destination position. The source S sends a Position Discovery Packet (PDP) packet to the nearest LCA in its zone using restricted directional flooding to inquire the LCA about the destination D position.

Upon receiving the first PDP the LCA checks whether the destination is in its zone or not. If yes, the destination is found in the authentication table of the LCA. So, the LCA will unicast a Position REPly (PREP) packet to the source. This PREP contains the destination position and passes back along the reverse path toward source.

If the destination is in another zone, the destination will not be found in the authentication table of the LCA. So the LCA sends multiple unicast PDP (using source routing) to the other LCAs in local zone and having adjacent LCAs in neighboring zones. Each LCA in that zone will send the PDP to its adjacent LCA in the neighboring zone. This PDP is sent using unicast if the adjacent LCA is reached in 1-hop. If the adjacent LCA is not within the transmission range of the first LCA, PDP is sent using restricted directional flooding.

These steps are repeated until the PDP packets reach LCAs having the destination node in their authentication tables. These LCAs, in turn, will unicast a PREP back along the reverse path to source. This packet is unicast through reverse path till reaching the source node, as shown in Figure 2. Table 4 summarizes the packets sent during the location service phase.

Figure 2 Authenticated location service

Table 4: Packets sent during the location service phase of ARANz

3.4 Route discovery, setup and maintenance

The needed steps to perform route discovery and setup are explained in this section. After receiving the destination position, the source starts with instantiating a route to the destination by sending a Route Discovery Packet (RDP). This is conducted using restricted directional flooding. Upon receiving the first RDP, the destination unicast a Route REPly (RREP) packet back via the reverse path to the source.

All the conducted route discovery steps are carried out using ARAN authentication steps. Each node along the RDP path and the reverse (REP) path validates the previous node signature, removes the previous node certificate and signature, signs the packet contents and attaches its own certificate. The only one difference between the behavior of the nodes upon receiving a request or a replay is that upon receiving a RDP a node records the previous node IP address and forwards sending the packet. On the other hand, when receiving a RREP it forwards the replay back to the predecessor from which it received the original request.

ARANz adopts on-demand routing approach, consequently, nodes keep track of whether routes are active or not. If no data is received on an existing route, the route is deactivated. Data received on an inactive route causes nodes to generate an ERRor (ERR) packet. Nodes also use ERR packets to report links in active routes that are broken due to node movement. All ERR packets are also signed.

Table 5 summarizes the packets exchanged during the route instantiation and maintenance phase.

Table 5: Packets sent during route instantiation and maintenance phase of ARANz

3.5 Data transmission

After finishing route instantiation, source initiates sending data to the destination. As in ARAN, only the control messages between nodes are signed and verified. Once the route reply reaches the originator, it is guaranteed that the discovered route is authentic. So, as in ARAN, data packets exchanged between nodes are not signed and do not include certificates. Accordingly, each node simply relays data packets to its successor in the route obtained during the route initiation process. Yet, to ensure the data privacy and prevent other trusted nodes from reading the data, it may be encrypted using the public key of the destination which the source can obtain during position discovery phase.

4. PERFORMANCE EVALUATION

In this section the performance of ARANz is studied and compared with existing protocols. Our protocol should be compared with the original ARAN protocol since our protocol is based on it. Besides, AODV protocol will also be considered for comparison issues since AODV is often considered as a benchmark for evaluating the Ad-Hoc routing protocols performance and as ARAN has been proposed based on it. We start this section with a summary of the properties of the discussed protocols. Then an analysis of their robustness in the presence of different attacks is provided in Subsection 4.2, while Subsection 4.3 provides a detailed simulated performance evaluation of the three routing protocols.

4.1 Summary of the evaluated protocols

Table 6 summarizes properties of the discussed protocols. Both AODV and ARAN are reactive topology-based routing protocols those use broadcasting in the route discovery process; while ARANz is a restricted directional flooding position-based routing protocol. AODV does not define any security requirements and trusts all participants. In contrast, ARAN and ARANz use cryptographic certificates to prevent most of the attacks against Ad-Hoc routing protocols and detect erratic behavior. Furthermore, ARANz aims to achieve high level of security and avoid single point of attack problem by distributing trust among several LCAs. All three protocols are loop-free and hence preserve the network resources and guarantee the correct operation. All of them also may be implemented at any network density.

AODV choses the minimum number of hops path. ARAN and ARANz do not guarantee the shortest path, but they offer the quickest path which is chosen by the RDP that reaches the destination first. Simulations result in [2] showed that the average path length for AODV and ARAN are almost the same. This indicates that even though ARAN does not explicitly seek shortest paths, the first route discovery packet to reach the destination usually passes along the shortest path. Hence ARAN is as effective as AODV in finding the shortest path. It is expected for ARANz to have the same criterion.

In ARAN each node should update its certificate from the trusted CA server; hence the load is centralized on that CA. This CA also presents a centralized trust and thus may be the system single point of attack. ARANz, on the contrary, tries to distribute load and trust by dividing the area into zones and introducing numerous LCAs in each zone. Thus, compromising one LCA will not prevent other LCAs from updating the certificates and electing a new LCA to replace the compromised one. Using multiple LCAs in ARANz, on the other hand, arises the need to keep them synchronized.

AODV and ARAN are more robust in the route discovery phase than ARANz since both broadcast the route request to the whole network. ARANz, though, uses restricted directional flooding to discover routes which may increase the effect of a failure or movement of a single node. After setting up the route the three protocols, roughly, have the same robustness since the failure of a node may result in packet loss and setting up a new route. ARANz tries to achieve higher robustness compared to ARAN by distributing trust among different LCAs; i.e., multiple LCAs should collaborate to issue certificates for the nodes inside a particular zone. Hence a failure of a single LCA (or even multiple LCAs) will not affect updating nodes' certificates since other LCAs in the zone are able to discover its failure and elect another LCA to replace it. However in ARAN the CA is a vital of the network and its failure prevents all other nodes from updating their certificates. After taking these points into consideration the robustness of AODV is considered high and those of ARAN and ARANz are considered as low and medium, respectively.

Table 6: Characteristics of the presented protocols [1]

4.2 ARAN and ARANz security analysis

Just like ARAN protocol, ARANz uses cryptographic certificates to prevent most of the security attacks that Ad-Hoc routing protocols face. It introduces authentication, message integrity and non-repudiation as part of a minimal security policy for the Ad-Hoc environment. Moreover, confidentiality in ARANz is ensured upon encrypting important data with the destination public key.

Since all ARAN packets must be signed, a node cannot participate in routing without authorization from the CA. Hence, this CA is a single point of attack and it is an important concern to keep this it uncompromised. In ARANz a node is allowed to participate in routing after gaining authorization from the LCAs of its local zone. Even in the case of one LCA compromise, the revocation mechanism used with ARANz may be executed to exclude this LCA from the network and elect a new one. One may suppose that introducing multiple LCAs may cause compromising the network if any LCA is compromised. However, as proofed in [1], security of the whole network is compromised only if three LCAs of a particular zone are compromised at the same time without being able to identify them as compromised. In this case these LCAs can collaborate together to issue certificates for untrusted nodes in their zone. Accordingly, a higher level of availability is achieved by ARANz due to avoiding single point of attack problem. On the other hand, the centralized CA in ARAN protocol results in lower availability since the compromise of this CA affects the security of the entire network.

The following is an analysis of the robustness of ARAN and ARANz in the presence of different attacks:

- Passive attacks: detecting passive attacks is very difficult since the operation of the network itself is not affected. One way of overcoming such problem is to use powerful encryption mechanisms to encrypt the data being transmitted, thus making it impossible for eavesdroppers to take advantage of the data overheard. Both ARAN and ARANz use cryptographic operations to guard control packets from eavesdropping.
- Active attacks: both protocols are robust against most active attacks such as:
  - Spoofed route signaling: all request packets, in ARAN as well as ARANz, are signed with the source private key and contain its certificate. Similarly, reply packets include the destination certificate and signature, ensuring that only the destination can respond to a particular request. Hence, impersonation attacks where either the source or destination is spoofed are prevented.
  - Fabricated routing messages: ARAN and ARANz do not prevent fabrication of routing messages, but they offer a precautionary step by ensuring non-repudiation since all routing messages must contain the sender certificate and signature. Therefore, a node that injects false messages into the network may be excluded from future route discovery processes.
  - Alteration of routing messages: both protocols assure that all fields of request and reply packets remain unchanged between source and destination. Since both packet types are signed by the initiating node, any alterations would be detected and the altered packet would be consequently discarded. Thus, modification attacks are prevented in both protocols.

Table 7 and Table 8 summarize the security requirements satisfied by both protocols as well as different attacks they defend against.

Table 7: ARAN and ARANz security analysis [1]

Table 8: ARAN and ARANz robustness against existing attacks [1]

4.3 Simulated network performance

GloMoSim is used as a simulation tool to evaluate the performance of AODV, ARAN and ARANz protocols. AODV is already implemented in GloMoSim, so two new models called “ARAN” and “ARANz” are added to GloMoSim to simulate ARAN protocol and our new protocol, respectively.

Nodes transmission range of 250m is simulated. The initial positions of the nodes are chosen randomly with node density of 60nodes/km^2. After that all nodes are allowed to move according to the random waypoint mobility model, i.e., each node travels to a randomly selected location at a configured speed and then pauses for a configured pause time, before choosing another random location and repeating the same steps.

802.11 MAC layer and Constant Bit Rate (CBR) traffic over User Datagram Protocol (UDP) have been used. Source and destination pairs are chosen randomly in both local and external communications. Five CBR sessions are simulated in each run. Each session generates 1000 data packets of 512 bytes each at the rate of 4 packets per second. Local communication percentage of 60% has been used, i.e., in each run three of the five CBR sessions are local and the other two are external. The motive behind choosing this percentage is that the chance for a node to communicate with a nearby node is higher than communicating to a faraway node.

For simulating ARAN and ARANz, we assumed that the key distribution procedure has been finished, so that all hosts can examine the genuineness of the signed packets. ARAN and ARANz are simulated using a 512-bit key and 16-byte signature. These values are reasonable to prevent compromise during the short time nodes spend away from the certificate authority and in the Ad-Hoc network [2].

For either protocol, a routing packet processing delay of 1ms is assumed. This value was obtained through field testing of the AODV protocol implementation in [3]. As well, a processing delay of 2.2 ms is added to account for the cryptographic operations for ARAN and ARANz. This value is adopted from [2] which they obtained through the implementation testing of measuring processing routing messages of ARAN for both a laptop and a handheld computer. A random delay between 0 and 10ms is introduced before the retransmission of a broadcast packet in order to minimize collisions.

The effect of five important parameters of Ad-Hoc networks have been tested. These parameters are nodes density, local communication percentage, zone size, failed nodes percentage, and malicious node percentage. For each parameter six performance metrics are evaluated. These metrics are:

1. Packet Delivery Fraction (PDF): fraction of data packets generated by the CBR sources and are received by intended destinations. This assesses the protocol ability to discover and maintain routes.
2. Average Path Number of Hops (APNH): average length of the discovered paths by a protocol. It is calculated by averaging the number of hops taken by different data packets to reach their destinations.
3. Packet Network Load (PNL): resulted overhead packets from constructing and maintaining network structure along with updating positions and certificates of nodes. It is calculated in ARANz as the total of all packets sent during the setup and maintenance phases. On the other hand, it is calculated in ARAN as the summation of packets sent to update nodes certificates. The transmission at each hop along the paths is also counted in this metric calculation. Related to AODV, it is a flat non-secure topology-based routing protocol; i.e., it has no network structure maintenance nor nodes positions or certificates update. Hence, PNL of AODV is excluded from the figures.
4. Packet Routing Load (PRL): ratio of routing packets to delivered data packets. Routing packets are those sent during the location service, route instantiation and route maintenance phases. The transmission at each hop along the route also is counted in this metric calculation.
5. Average Route Acquisition Latency (ARAL): average delay for discovering a route to a destination. It is defined in ARAN and AODV as the average delay between sending a route discovery packet by a source and receiving the first analogous route reply packet. In ARANz, it is defined as the average delay for both discovering position of the destination and initiating a route to it.
6. Average End-to-End Delay of data packets (AEED): The average delay between the sending of data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all delays caused during position inquiry, route establishment, buffering and processing at intermediate nodes and retransmission delays at the MAC layer.

For the following figures, each point is an average of five simulation runs with identical configuration but different randomly generated numbers.

The details of the conducted experiments to study the effect of node mobility speed and area size can be found in [1]. Results in [1] showed that ARANz is highly effective in discovering and maintaining routes for delivery of data packets even with relatively high node mobility. Even though ARANz does not explicitly seek shortest paths, the first RDP to reach the destination usually travels along the shortest path. Hence, ARANz is highly efficient in discovering shortest paths. On the other hand, PNL for ARANz increases slightly as the nodes mobility speed increases. Frequent nodes mobility results in increasing number of packets sent for updating nodes positions as well as electing new LCAs.

Upon studying the area size effect, results showed that PDF decreases with increasing the area size due to higher number of nodes the packet passes through which increases the probability of link break. APNH of the discovered paths increases with increasing the area size, due to higher number of nodes the packet passes through if the source and destination are apart from each other, which means longer paths. PRL for the three protocols increases with increasing area size due to higher probability of link break that requires reinitiating a RDP. However, ARANz still has the minimum packet routing load as a result of using restricted directional flooding in forwarding RDP. ARAL for the three protocols increases with increasing area size due to increasing number of nodes that the control packets pass through. Moreover, larger network size results in increasing number of packets sent for updating nodes' positions and certificates.

4.3.1 Node Density Effect

To test the effect of node density, a 2km×2km network that is divided into 4 zones is considered. Nodes inside this network move at a maximum speed of 5m/s. Five CBR sessions are simulated in each run, three of them are local and two are external. Simulations are run with 40 nodes/km^2, 60 nodes/km^2, 80 nodes/km^2 and 100 nodes/km^2.

As Figure 3(a) shows, higher PDF for all protocols is obtained for node density values between 60 nodes/km^2 and 80 nodes/km^2. As density decreases below 60 nodes/km^2, the probability of finding a path between the source and destination decreases. On the other hand, as density increases above 80 nodes/km^2, the number of nodes participating in rebroadcasting the control packets increases. In other words, an intermediate node receives multiple copies of the same RDP packet from its neighbours. Processing these control packets may cause delay in processing data packets as well as causing some packet drops. However, Figure 3(a) shows that the PDF for all protocols is above 93% for all simulated node density values. This suggests that the three protocols are highly effective in discovering and maintaining routes for delivery of data packets regardless of node density.

Figure 3: Node Density Effect

It is clear from Figure 3(b) that the APNH decreases with increasing the node density, until reaching its minimum values at node densities ranging from 60 nodes/km^2 to 80 nodes/km^2. This suggests that increasing the node density increases the chance to find faster/shorter path until reaching 80 nodes/km^2. As density increases above 80 nodes/km^2 APNH starts to increase. This indicates that increasing the density more than 80 nodes/km^2 will only make the nodes closer to each other while not serving in finding shorter paths. In fact, increasing the number of control packets received from the neighbours may result in dropping some control packets that may have already passed through the shortest path. However, the differences in APNH between the three protocols and for each protocol separately are insignificant. This is an indication that the three protocols are efficient in discovering the shortest paths regardless of node density.

Figure 3(c) shows that the PNL for ARAN is significantly higher than ARANz. Moreover, this figure shows that PNL for both ARAN and ARANz increase as the node density increases due to increasing the number of nodes updating their certificates and positions. However, the increase in these metrics is more significant upon simulating ARAN protocol. This large difference results from ARAN broadcasting certificate update request packets to the entire network. On the other hand, ARANz sends packets related to updating nodes' positions and certificates only to the nearest LCA.

It is conspicuous from Figure 3 (d) that the PRL for the three protocols slightly increase as the node density increases, due to the larger number of nodes receiving and broadcasting RDP packets. ARANz has the minimum PRL as a result of using restricted directional flooding in sending RDP packets.

Figure 3(e) shows that the ARAL for the three protocols increase with increasing node density. This increase is a result of the increased number of nodes participating in broadcasting RDP packets, which causes congestion as well as delay in processing control packets.

ARAL for ARAN and ARANz protocols is higher than AODV due to digital signature generation and verification. Also, ARAL for ARANz is higher than that for ARAN due to time required to get the destination node position.

Figure 3(f) demonstrates that AEED curves for the three protocols are almost identical to each other. Although ARAN and ARANz have higher ARAL, the number of route discoveries and position enquiries performed is a small fraction of the number of data packets delivered. Hence, the effect of ARAL on AEED of the data packets is insignificant. Moreover, the AEED for the three protocols is not affected by increasing node density.

4.3.2 Local Communication Effect

To evaluate our protocol considering local communication percentage, a 2km×2km network which is divided into 4 zones is considered. A total of 240 nodes are randomly placed in this network. These nodes are allowed to move at 5m/s speed. Five CBR sessions are simulated in each run. Simulations are run with 0%, 40%, 60% and 100% local communication. These percentages are adjusted by specifying the local and external CBR sessions. For example, to simulate 40% local communication, two of the CBR sessions are chosen as local and the other three are external.

As shown in Figure 4(a), PDF obtained using either protocol slightly increases as the percentage of local communication increases and nearly reaches 100% when all communications are local. Larger percentage of local communications means shorter paths, i.e. lower probability of having link breakage and data packet drops. Moreover, it is clear from the figure that PDF obtained for either protocol is above 96% in all scenarios. This suggests that the three protocols are highly effective in discovering and maintaining routes for delivery of data packets.

Figure 4: Local Communication Effect

Figure 4(b) shows that ARAN and ARANz are as efficient as AODV in discovering the shortest paths regardless of the simulated local communication percentage. The same figure indicates that APNH slightly decreases for all protocols with increasing local communication because the source and destination nodes are closer to each other.

Figure 4(c) shows that the PNL for both protocols are not affected by local communication percentage because the packets sent for updating nodes certificates and maintaining network structure are sent regardless of the number and type of communication sessions among nodes. Figure also shows that PNL for ARANz is still much less than this for ARAN.

Figure 4(d) shows that the PRL curves for the three protocols slightly decrease as the local communication increases due to the shorter paths. Shorter paths decrease the probability of link break, which in turn, reduces the need for reinitiating a new RDP packet. The figure shows that ARANz PRL is significantly lower than the other two protocols, since ARANz does not broadcast the RDP packet to the whole network, instead, it is sent using restricted directional flooding. It is also clear from Figure 4(d) that ARAN has higher PRL than AODV. As discussed earlier, this difference results as a consequence of higher packets processing and authentication delay in ARAN along with the possibility of sending RREP packets by the intermediate nodes in AODV.

As expected, Figure 4(e) shows that AODV is superior in its ARAL as it has the shortest processing delay at each node. Moreover, ARANz has the highest ARAL because ARANz needs to carry out a position discovery step. However, ARANz ARAL improves rapidly as more and more packets become internal ones because the nearest LCA, upon receiving a PDP packet, will find the destination in its authentication table, so there is no need to communicate with LCAs in other zones. In fact, all protocols have better ARAL as more packets are delivered locally due to shorter paths although ARAL curves of AODV and ARAN decrease at a slower rate compared to ARANz. The reason behind this difference is that the RDP packets in AODV and ARAN are flooded to the whole area even if the communications are local. This flooding affects ARAL for other external communications by increasing the processing delay of other RDP packets.

Figure 4(f) shows that AEED slightly decreases with increasing local communication due to the shorter paths whether for data or control packets.

4.3.3 Zone Size Effect

To examine the effect of zone size, two networks of 3km×3km and 2km×2km are considered and divided into multiple zones as discussed in the following two sections.

4.3.3.1 Zone Size Effect Considering 3km×3km Network

In this scenario, a network of 3km×3km is considered. This network contains 540 nodes, i.e. the node density is 60 nodes/km^2. The nodes move at a maximum speed of 5m/s. Five CBR sessions are simulated in each run, three of them are local and two are external. The network is divided into 1 zone of 3km×3km, 4 zones each of 1.5km×1.5km, 9 zones each of 1km×1km and finally 16 zones each of 750m×750m.

By looking at Figure 5(a through f), it is clear that ARAN and AODV are not affected by changing zone size since only ARANz deals with the network as zones. Accordingly, only ARANz protocol is considered in the following discussion.

Figure 5(a) shows that ARANz PDF is always above 96%. This is an indication that ARANz, just like ARAN and AODV, is highly effective in discovering and maintaining routes regardless of zone size.

Figure 5(b) shows that APNH for ARANz is identical to that for the other two protocols, suggesting that ARANz is as efficient as the other two protocols in discovering the shortest paths regardless zone size.

Referring to Figure 5(c), it is clear that PNL for ARANz increases as the zone size increases. This is because packets sent for updating nodes certificates and maintaining the network structure are sent using restricted directional flooding towards the nearest LCA to the node, i.e. as the distance between the node and the nearest LCA increases, the number of nodes participating in forwarding these packets also increases.

Figure 5(d) shows that the PRL for ARANz slightly decreases with increasing the zone size. This is because dividing the area into multiple zones reduces the probability of finding the destination in the authentication table of the nearest LCA, therefore, the PRL increases due to communicating

LCAs in other zones. However, in the case of dealing with the network as one zone, the nearest LCA upon receiving PDP packet finds the destination in its authentication table, so there is no need to communicate other LCAs.

Figure 5: Zone Size Effect Considering 3km×3km Network

Figure 5(e) shows that ARAL for ARANz significantly decreases as the zone size increases. The highest ARAL is obtained in the case of 750m×750m zone size due to time required for communicating LCAs in other zones to inquiry about the destination position. Figure 5(f) shows that ARANz AEED is almost not affected by changing zone size. As mentioned previously, the number of route and position discoveries is a small fraction of the number of data packets delivered. Hence the effect of ARAL on AEED is unnoticeable.

It is conspicuous from the analysis that a better performance (significantly reduced PNL) is obtained for ARANz upon using a small zone size. On the other hand, PRL slightly decreases and ARAL significantly decreases as the zone size increases. Hence a moderate performance in terms of the three metrics is obtained upon dividing the area into four 1.5km×1.5km or nine 1km×1km zones.

4.3.3.2 Zone Size Effect Considering 2km×2km Network

To ensure the results obtained in the first scenario, another simulation scenario is carried out. In other words, the aim of this scenario is to ensure whether a moderate performance is obtained upon dividing the area into four or nine zones, or upon using 1.5km×1.5km or 1km×1km zone size.

In this scenario, a network size of 2km×2km, a node density of 60 nodes/km^2 and a maximum mobility speed of 5m/s are considered. Three local and two external CBR sessions are simulated. The network is divided into 1 zone of 2km×2km, 4 zones each of 1km×1km, 9 zones each of 666.666m×666.666m and finally 16 zones each of 500m×500m.

Looking at Figure 6(a through f), it is clear that the PNL for ARANz significantly decreases with decreasing the zone size (increasing the number of zones). On the other hand, the PRL slightly decreases and the ARAL significantly decreases with increasing the zone size (decreasing the number of zones). Thus a moderate performance regarding the five metrics is obtained upon dividing the area into four 1km×1km or nine 666.666m×666.666m zones.

From the results of the two scenarios we can conclude that regardless of the network size, a moderate performance regarding the three metrics is obtained upon dividing the area into 4 or 9 zones.

Figure 6 Zone Size Effect Considering 2km×2km Network

4.3.4 Node Failure Percentage Effect

In the previously studied scenarios, all participating nodes are assumed as well-functioning. In this section, we try to inspect our protocol efficiency and compare it with AODV and ARAN protocols, in case of having some malfunctioning (failed) nodes.

To examine the effect of node failure percentage a 2km×2km network that is divided into 4 zones is considered. The nodes inside this network move at a maximum speed of 5m/s. Five CBR sessions are simulated in each run, three of them are local and two are external. Simulations are run with 0%, 10%, 20% and 40% node failure percentages.

To simulate the node failure, a node periodically draws a random number between 0 and 1. If the drawn number is less than the failure probability, then the node deletes all information about the zone it is residing in and becomes unable to participate in the network activities. Node failure continues until a randomly chosen period between 10s and 60s. By the end of this period, the failed node is placed at a random place in the simulation area. After that, the recovered node starts communicating with LCAs in the new zone so that it is issued a fresh certificate and re-joins the network.

Figure 7(a) shows that the PDF for the three simulated protocols decreases as the node failure percentage increases. A higher node failure percentage leads to a higher probability of having link break resulting in dropping some data packets and reinitiating RDP packets. The probability of link breakage is significantly higher for ARANz and ARAN due to higher packet processing and authentication delay at each node. The situation becomes worse in ARAN protocol if the failed node is the CA itself. In this case, all other nodes are unable to update their certificates and take part in sending data packets, resulting in dropping some packets. In ARANz, however, only nodes inside a particular zone will not be able to update their certificates upon the failure of the four LCAs in that zone at the same time.

It is apparent from Figure 7(b) that the APNH increases slightly with increasing node failure percentage. Higher node failure percentage means higher probability of link breakage and the select of alternate non-optimal paths, increasing APNH. Figure 7(c) shows that the PNL for both protocols (ARAN and ARANz) slightly decreases as the node failure percentage increases. This decrease in PNL is due to the decrease in the number of nodes updating their certificates and positions as a result of their failure.

Figure 7(d) shows that PRL increases for the three protocols as the node failure percentage increases. The reason behind this increase is the need to reinitiate RDP packets subsequent to link breaks resulting from nodes failure. ARANz still has the minimum PRL in all experiments due to sending RDP packets using restricted directional flooding towards the destination. On the other hand, ARAN protocol has the maximum (worst) PRL. ARAN has a high probability of link breakage due to the high packet processing and authentication delay at each node. Increased number of failed nodes results in resending RDP packets several times in an attempt to secure a route between the communicating nodes, resulting in higher PRL. Moreover, a worse case may appear in ARAN protocol if the CA itself malfunctions. In this case, other nodes will not be able to update their certificates nor participate in constructing a route between the source and destination nodes.

By looking at Figure 7(e), it is clear that ARAL for the three protocols slightly increases as the node failure percentage increases. Higher node failure percentage means higher link break probability and the select of alternate non-optimal paths leading to higher delay in processing control packets. On the other hand, AEED is almost identical for the three protocols (refer to Figure 7(f)). The effect of ARAL on AEED of data packets is not significant since the number of the performed route discoveries and position enquiries is a small fraction of the sent data packets.

5. RESULTS SUMMARY AND DISCUSSION

AODV is a non-secure reactive routing protocol; hence it has less processing overhead compared to ARAN and ARANz since nodes in AODV don't apply cryptographic operations such as validating the previous node signature, signing the routing packets and appending certificates. AODV uses broadcasting in the route discovery phase which increases its robustness against nodes' failure on one hand, while on the other hand it increases packet overhead. This is because the route request packet is sent to all nodes in the network. Due to this, AODV is not a scalable protocol.

ARAN is a reactive routing protocol that uses broadcasting in the route discovery process. ARAN uses cryptographic certificates to prevent most of the attacks against Ad-Hoc routing protocols as well as to detect erratic behaviours such as the use of invalid certificates, improperly signed packets and misuse of some packets. However using these certificates increases the route acquisition latency along with packet and processing overheads compared to AODV. These increased latency and overhead are due to the encryption/decryption processes together with route request broadcast. ARAN also suffers from the centralized trust and load, i.e.; single point of attack and failure. Similar to AODV, ARAN has scalability problem due to using one certificate authority server which can be the operation bottleneck.

With ARANz, a scalable and secure solution is achieved. Adopting the authentication methods used in ARAN, ARANz is a secure routing protocol. Furthermore, by dealing with the network as zones and using restricted directional flooding, ARANz aims to show better scalability and performance. As opposite to ARAN, ARANz distributes load and trust by dividing the area into zones and introducing multiple certification authorities (i.e. Local CAs (LCAs)) in each zone. Distributing load and trust helps in achieving high level of security and robustness by avoiding single point of attack and failure problems. Using multiple LCAs in ARANz, on the other hand, comes up with a need to keep them synchronized.

From the obtained simulation results, presented in the previous section, many points are concluded. These points are summarized as follows:

- PDF for the three protocols is above 95% in most scenarios. This indicates that the three protocols are highly effective in discovering and maintaining routes for delivery of data packets even with relatively high node mobility and large area networks. Upon studying the effect of malicious node percentage, however, results show that the decrease in PDF is much slower in ARANz in most cases, implying that ARANz is efficient in detecting and isolating malicious nodes even with relatively large percentage of them.
- PNL for ARANz is significantly less than ARAN. The main reason behind this gap is that nodes in ARAN are unaware of the position of the CA server, hence, all certificate update request packets sent from nodes to CA are broadcast to the entire network. In ARANz, however, most packets are sent using restricted

directional flooding, source routing, zone flooding or LCA flooding.

- ARANz has the minimum PRL in all experiments and the conducted statistical analysis tests confirm that the differences between PRL for the three protocols are statistically significant. In contrast to AODV and ARAN, ARANz does not broadcast the RDP packets to the whole area, instead, these packets are sent using restricted directional flooding towards the destination. Even PDP packets are sent using restricted directional flooding or source routing. Hence, PDP packets do not significantly affect PRL, especially if the source and destination are in the same zone.
- ARAN has higher PRL compared to AODV as a consequence of higher packet processing and authentication delay in ARAN protocol. In other words, higher delay increases the chance of having link break and reinitiating RDP packets, i.e. higher PRL.
- APNH is almost identical for the three protocols for a specified network parameters setting. In other words, even though ARAN and ARANz do not explicitly seek the shortest paths, the first RDP packet to reach the destination usually travels along the shortest path. Hence, it is obvious that ARAN and ARANz are as efficient as AODV in discovering shortest paths.
- AODV is superior in its ARAL as it has the shortest processing delay at each node. On the other hand, while processing routing control packets in ARAN and ARANz, each node has to verify the digital signature of the previous node and replace this signature with its own digital signature, in addition to the normal packet processing done by AODV. This signature generation and verification results in additional delay at each hop, and so ARAL increases. Moreover, ARANz has the highest ARAL since it needs to carry out a destination position discovery step. However, ARANz ARAL improves rapidly as more and more packets become internal ones. Upon increasing local communications, ARANz ARAL significantly decreases since the position of the destination is found in the authentication table of the nearest LCA to the source, so there is no need to communicate with LCAs in other zones.
- Differences in AEED between the three protocols are almost negligible since the number of route discoveries and position enquiries performed is limited compared to the number of data packets delivered. Hence, the effect of ARAL on AEED of data packets is not significant.
- High PDF and low APNH for all protocols are obtained for node density values between 60 nodes/km^2 and 80 nodes/km^2. However, PDF for all protocols is above 93% for all simulated node density values. Moreover, results of the conducted statistical analysis tests show that the differences in APNH between the three protocols and for each protocol separately are statistically insignificant. This suggests that the three protocols are highly effective in discovering and maintaining the shortest routes regardless of node density.
- Better performance in terms of PNL is obtained upon decreasing the zone size (increasing the number of zones). Decreasing the zone size results in decreasing the distance between the node and the nearest LCA, and accordingly, decreasing the number of nodes participating in forwarding the packets needed for updating nodes certificates and maintaining the network structure, i.e. significantly decreasing PNL. On the other hand, better performance in terms of PRL and ARAL is obtained with increasing the zone size (decreasing the number of zones). Increasing the zone size results in increasing the probability that the nearest LCA, upon receiving PDP, finds the destination in its authentication table. So, there is no need to communicate other LCAs, i.e. PRL slightly decreases and ARAL significantly decreases as the zone size increases. Accordingly, a moderate performance in terms of the three metrics is obtained upon dividing the area into four or nine zones.
- A higher node failure percentage results in a significant decrease in PDF and a slight increase in PRL for the three tested protocols, since a higher probability of link break results in dropping some data packets, reinitiating RDP packets as well as selecting non-optimal paths. ARANz and ARAN protocols robustness against node failure is less than that for AODV due to having some nodes, such as LCAs in ARANz and centralized CA in ARAN, whose failure may affect other nodes in the network. The situation is worse in ARAN protocol, as if the CA is corrupted all other nodes will neither be able to update their certificates nor participate in the network operations. In ARANz however, only nodes inside a particular zone will not be capable of updating their certificates upon the failure of the four LCAs in that zone. Results of the conducted statistical analysis tests indicate that the increase in PNL for ARAN is more

significant than AODV and ARANz, assuring that AODV and ARANz are more stable against node failure percentage.

As a summary, the simulation results illustrate the efficiency of the three protocols in discovering and maintaining not only routes, but also the shortest paths. The results suggest that ARANz has achieved the scalability issue by maintaining the minimum packet routing load even with large networks and high node mobility. ARANz reduced packet routing load is a normal result of using restricted directional flooding to send RDP packets. The cost of ARAN and ARANz security is higher routing load and latency in the route discovery process due to cryptographic computation that must occur. Moreover, ARANz reduced packet routing load comes in the price of higher latency in the route discovery due to the time required to obtain destination position.

6. CONCLUSIONS

ARANz routing protocol addresses the managed-open environment in which the possibility of utilizing already established infrastructure is available. ARANz proposes a hierarchal and distributed routing procedure, which aims to improve the routing protocol performance and scalability via dividing the area into zones. ARANz aims to achieve robustness, increase network security and solve the single point of failure and attack problems by introducing numerous LCAs. Our ARANz also seeks to exhibit better scalability, performance and robustness through utilizing position-based routing.

In this work, a detailed performance evaluation has been conducted. Our simulations show that ARANz is highly effective in discovering the shortest paths and keeping secure routes even with relatively high node mobility, large network size, different node densities, different local communication percentages, and different zone sizes.

ARANz is still able to have superior performance even with having large percentage of malfunctioning (failed) nodes. Moreover, ARANz has achieved the scalability issue by maintaining the minimum packet routing load in all presented scenarios compared to AODV and ARAN protocols. The cost of ARANz is higher latency in route discovery on account of the time required for authentication and packet processing along with obtaining destination position.

7. FUTURE WORKS

Our next task is to evaluate the effectiveness of ARANz in dealing with security issues considering the existence of malicious nodes performing different types of attacks. We also aim to test ARANz scalability considering different number and positions of LCAs in each zone, in addition to studying the effect of using different zone shapes. Comparisons will then be performed with other existing secure routing protocols especially secure AODV extensions. Finally, in our current work, we have considered that nodes are evenly geographically distributed. Hence it is an important issue to consider the case when some regions of the network have very few nodes and some others have much more.

REFERENCES

[1] Qabajeh L, Mat Kiah ML and Qabajeh M. A more secure and scalable routing protocol for mobile ad hoc networks. *Security and Communication Networks*, 2013; 6(3):286-308.

[2] Sanzgiri K, LaFlamme D, Dahill B, Levine B, Shields C and Belding-Royer E. Authenticated Routing for Ad Hoc Networks. *IEEE Journal On Selected Areas In Communications*, 2005; 23(3):598-610.

[3] Perkins C and Royer E. Ad hoc on-demand distance vector routing. *Proceedings of The 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999, New Orleans, USA; 90-100.

[4] Beijar N. Zone Routing Protocol (ZRP). 1998. Networking Laboratory, Helsinki University of Technology, Finland. http://www.netlab.hut.fi/opetus/s38030/k02/Papers/08-Nicklas.pdf

[5] Lin T. Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications 2004. Ph.D. thesis, Faculty of the Virginia Polytechnic Institute and State University, Blacksburg, Virginia. http://scholar.lib.vt.edu/theses/available/etd-03262004-44048/unrestricted/Tao_PhD_Dissertation.pdf

[6] Abolhasan M, Wysocki T and Dutkiewicz E. A review of routing protocols for mobile ad hoc networks. *Elsevier Ad Hoc Networks*, 2004; 2(1):1-22.

[7] Cao Y and Xie S. A Position Based Beaconless Routing Algorithm for Mobile Ad hoc Networks. *Proceedings of The IEEE*

International Conference on Communications Circuits and Systems, 2005, Hong Kong, China; 303-307.

[8] Li H and Singhal M. A Secure Routing Protocol for Wireless Ad Hoc Networks. *Proceedings of The 39th IEEE Annual Hawaii International Conference on System Sciences*, 2006, Hawaii, USA; 225a-225a.

[9] Mizanur Rahman Sk, Mambo M, Inomata A and Okamoto E. An Anonymous On-Demand Position-based Routing in Mobile Ad Hoc Networks. *Proceedings of The International Symposium on Applications and the Internet,* 2006, Arizona, USA; 300-306.

[10] Zapata M. Secure Ad hoc On-Demand Distance Vector Routing. *ACM Mobile Computing and Communications Review*, 2002; 6(3):106-107.

[11] Li Q, Zhao M, Walker J, Hu Y, Perrig A and Trappe W. SEAR: A Secure Efficient Ad Hoc On Demand Routing Protocol for Wireless Networks. *Security and Communication Networks*, 2009; 2(4):325-340.

[12] Ali M, Ullah Z, Khan M and Hafeez A. Secure and Efficient Routing Mechanism in Mobile Ad-Hoc Networks. *International Journal Of Advanced Computer Science And Applications*, 2018; 9(4): 436-441.

[13] Belgaum M, Musa1 Sh, Su'ud M, Alam M, Soomro S and Alansari Z. Secured Approach towards Reactive Routing Protocols Using Triple Factor in Mobile Ad Hoc Networks. *Annals of Emerging Technologies in Computing (AETiC)*, 2019; 3(2):32-40.

[14] Moudni H, Er-rouidi M, Mouncif H and Hadadi B. Secure routing protocols for mobile ad hoc networks. *International Conference on Information Technology for Organizations Development (IT4OD)*, 2016; 1-7.

[15] Saoud, B and Moussaoui, A. New Routing Protocol in Ad Hoc Networks. *International Conference on Computer Networks and Inventive Communication Technologies (ICCNCT)*, 2019; 443-452.

[16] Iche A and Dhage M. Location based Routing Protocols: A Survey. *International Journal of Computer Applications*, 2015; 109(11):28-31.

[17] Karp B, Kung H. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. *Proceedings of The 6th ACM/IEEE Annual International Conference on Mobile Computing and Networking*, 2000, Massachusetts, USA; 243-254.

[18] Wu X. VPDS: Virtual Home Region based Distributed Position Service in Mobile Ad Hoc Networks. *Proceedings of The 25th IEEE International Conference on Distributed Computing Systems*, 2005, Ohio, USA; 113-122.

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

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

[21] Qabajeh L, Mat Kiah ML and Qabajeh M. Secure Unicast Position-based Routing Protocols for Ad-Hoc Networks. *Acta Polytechnica Hungarica*, 2011; 8(6):191-214.

[22] Shen H and Zhao L. ALERT: an anonymous location-based efficient routing protocol in MANETs. *IEEE transactions on mobile computing*, 2013; 12(6):1079-1093.

[23] Song J, Wong V and Leung V. Secure position-based routing protocol for mobile ad hoc networks. *Elsevier Ad Hoc Networks Journal*, 2007; 5(1):76-86.

Table 1 Packet identifiers for ARANz

Packet identifier	**Stand for**	**Packet identifier**	**Stand for**
NETSET	NETwork SETup	NIN	Node INformation
NROLE	Node ROLE	CREQ	Certificate REQuest
ACREQ	Acceptance of Certificate REQuest	ACREP	Acceptance for Certificate REPly
CREP	Certificate REPly	NCERT	Node CERTificate
DNODE	Departed NODE	NNODE	New NODE
NZONE	New ZONE	NLCAP	New LCA Position
NALCAP	New Adjacent LCA Position	NLCAE	New LCA Election
NPROB	Node PROBability	FLCA	Failed LCA
FALCA	Failed Adjacent LCA	NLCA	New LCA
NALCA	New Adjacent LCA	FNODE	Failed NODE
EZONE	Empty ZONE	MNODE	Misbehaviour NODE
CNODE	Compromised NODE	PDP	Position Discovery Packet
PREP	Position REPly	RDP	Route Discovery Packet
RREP	Route REPly	ERR	ERRor

Table 2: Packets sent during the network setup phase of ARANz

Pid	**Stand for**	**Description**	**From**	**To**
NETSET	NETwork SETup	• Sent to notify nodes currently in the network of initiating the network setup phase and collecting information about these nodes. • Signed using KNET- so that nodes can make sure that the PCA is actually the node that has sent the packet.	PCA	All non-PCA
NIN	Node INformation	• Contains information about the source node such as position, speed, battery remaining life time, CPU power and memory. • Encrypted and decrypted using CK to ensure that this packet is forwarded by authorized nodes only. • Sent through the reverse path of the NETSET packet until reaching PCA.	All non-PCA	PCA
NROLE	Node ROLE	• A particular message is unicast to each participant node using source routing, containing the initial role (LCA or regular node) that this node will play.	PCA	All non-PCA

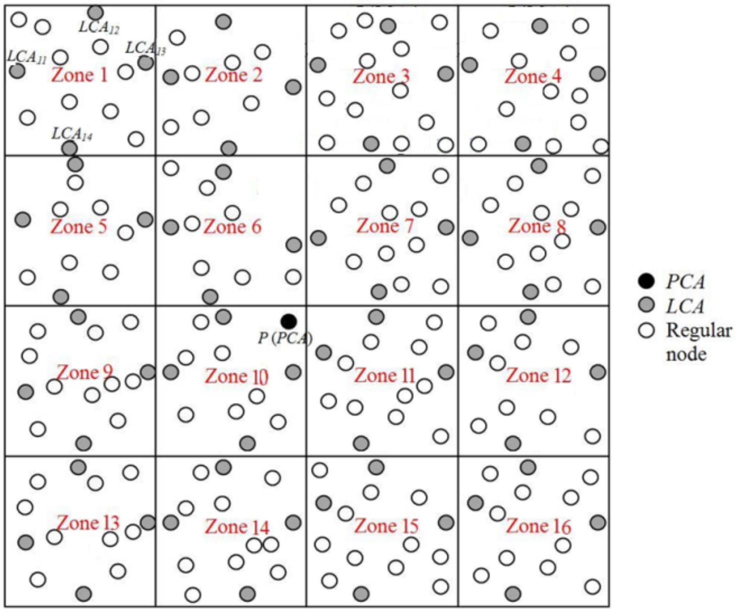


Figure 1 Network structure after electing initial LCAs

Table 3 Packets sent during the network maintenance phase of ARANz

Case	**Pid**	**Stand for**	**Description**	**From**	**To**
Certificate update	CREQ	Certificate REQuest	• Sent periodically requesting to update the certificate of node *n*. • Sent using restricted directional flooding.	Each regular node n	Nearest LCA in its zone
	CREP	Certificate REPly	• Contains the updated certificate of node *n*. • Sent through the reverse path of the *CREQ*.	Nearest LCA to n	Node n
	ACREQ	Acceptance of Certificate REQuest	• Sent to ask whether to update the certificate for *n* or not. • Sent using source routing.	Nearest LCA to n	Other LCAs in the zone
	ACREP	Acceptance of Certificate REPly	• Sent in the case of accepting the certificate update request. • Sent through the reverse path of the *ACREQ*.	Other LCAs in the zone	Nearest LCA to n
	NCERT	Node CERTificate	• Contains the newly issued certificate to enable zone *LCAs* to store identical information. • Sent using source routing.	Nearest LCA to n	Other LCAs in the zone
Node mobility	UNPOS	Update Node POSition	• Contains the new position of a node *n* that has moved a pre-defined distance (*Dmov*) from its last known position. • Sent using restricted directional flooding.	Moving node	Nearest LCA to n
	DNODE	Departing NODE	• Sent when a node *n* departs to a neighbouring zone to indicate that this node is trusted and contains the node position. • Sent using one-hop unicast if the adjacent *LCA* is within the transmission range of the departed zone *LCA*, else restricted directional flooding is used.	Nearest LCA to the zone that node n is departing to	Adjacent LCA in the neighbouring zone
	NNODE	New NODE	• Contains information about the new node. • Sent using source routing.	Adjacent LCA in the new zone	Other LCAs in its zone
	NZONE	New ZONE	• Contains the number and public key of the new zone as well as *IP* addresses and positions of the zone *LCA*s. • Sent using source routing.	Adjacent LCA in the new zone	Departing node n
	ULPOS	Update LCA POSition	• Contains the new position of a *LCA* that has moved *Dmov* from its last known position. • Sent using zone flooding.	Moving LCA	All nodes in its zone
	UALPOS	Update Adjacent LCA POSition	• Contains the new position of a *LCA* that has moved *Dmov* from its last known position. • Sent using one-hop unicast or restricted directional flooding.	Moving LCA	Adjacent LCA
	NLCAE	New LCA Election	• Sent to initiate a new *LCA* election if a *LCA* has decided to depart its zone *z*, or its distance from the middle point of the zone boundary became higher than a pre-defined distance (*Dsid*). • Sent using zone flooding.	Departing LCA	All nodes in zone z
LCA synchronization	CLSYN	CLocks SYNchronization	• Sent periodically (each pre-defined time *Tls*) and contains a timestamp to help *LCA*s keep synchronized clocks. To increase the system robustness, *LCA*s alternate this job. • Sent using *LCA* flooding.	Any LCA	All LCAs in the network

Table 3 Packets sent during the network maintenance phase of ARANz (continued)

Case	Pid	Stand for	Description	From	To
Node failure	FLCA	Failed LCA	• Sent to initiate a new *LCA* election in the case of sudden *LCA* failure which is discovered if other *LCA*s in the zone *z* do not receive the *ACREQ* packet from the failed *LCA* in a pre-determined time (*Tcu*). • Sent using zone flooding.	One of the other LCAs in zone z (voluntary LCA)	All nodes in zone z
	FALCA	Failed Adjacent LCA	• Sent to inform the adjacent *LCA* about the failed *LCA*. • Sent using restricted directional flooding.	Voluntary LCA	Adjacent LCA of the failed one
	FNODE	Failed NODE	• Contains the *IP* address and public key of a failed node n to enable it to join the network from any zone. • Sent using *LCA* flooding, i.e. using source routing between *LCA*s in the same zone and using one-hop unicast or restricted directional flooding between adjacent *LCA*s.	LCA that issued the last certificate for n (if n is a regular node) or voluntary LCA (if n is a LCA)	All LCAs in the network
LCA election	NPROB	Node PROBability	• Contains the probability of a node in the corresponding zone z to replace the departing (or failed) *LCA*. • Sent through the reverse path of the *NLCAE* (or *FLCA*).	All nodes in zone z	Departing (or voluntary) LCA
	NLCA	New LCA	• Contains the *IP* address and position of the new *LCA*. • Sent using zone flooding.	Departing (or voluntary) LCA	All nodes in zone z
	NALCA	New Adjacent LCA	• Contains the *IP* address and position of the new *LCA*. • Sent using one-hop unicast or restricted directional flooding.	Departing (or voluntary) LCA	Adjacent LCA
Empty zone	EZONE	Empty ZONE	• Sent to inform *LCA*s of the 8-neighbouring zones that this zone will be empty. • Sent between *LCA*s in the same zone using source routing and between adjacent *LCA*s using one-hop unicast or restricted directional flooding.	Last node n leaving a particular zone z1	LCAs of the 8-neighbour zones of z1
	PKPREQ	Zone Private Key Part REQuest	• Sent when a node leaves zone *z2* and enters an empty zone *z1*. • Sent to request the empty zone private key parts that the 4 adjacent *LCA*s have. • Sent using one-hop unicast or restricted directional flooding.	Nearest LCA in z2	4 adjacent LCAs of z1
	PKPREP	Zone Private Key Part REPly	• Contains the empty zone private key part they have. • Sent through the reverse path of the *PKPREQ*.	4 adjacent LCAs of z1	Nearest LCA in z2
	SNODE	Sole NODE	• Sent upon receiving and combining the private key parts. • Sent to inform *n* that it is the only node in the zone and giving it the needed information. • Sent using one-hop unicast or restricted directional flooding.	Nearest LCA in z2	node n

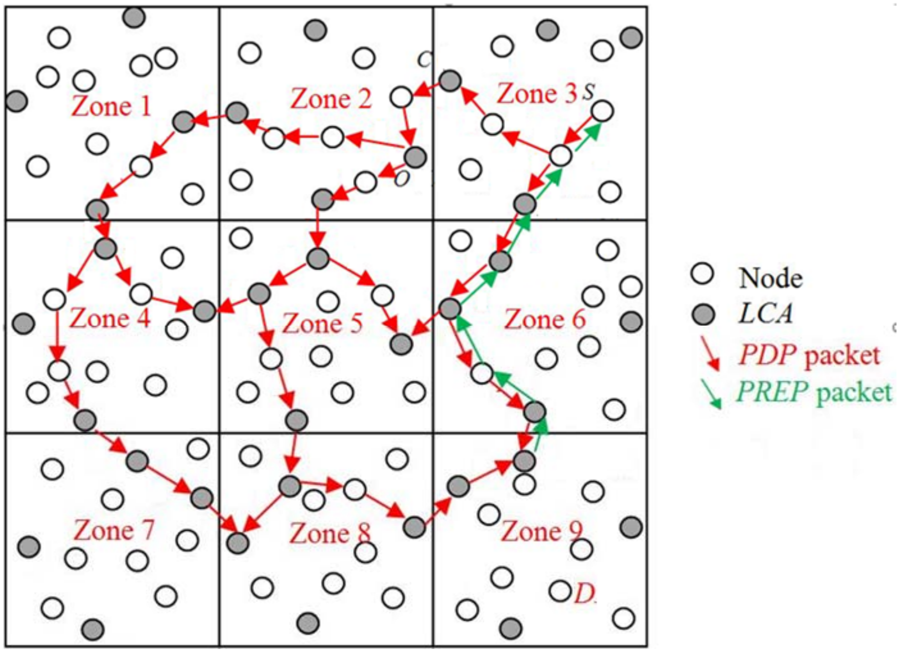


Figure 2: Authenticated location service

Table 4: Packets sent during the location service phase of ARANz

Pid	Stand for	Description	From	To
PDP	Position Discovery Packet	• Initiated to ask for the position of destination D. • Sent using restricted directional flooding or source routing.	Source node S	Nearest LCA in its zone (or all LCAs having adjacent LCA in case of external communications)
PREP	Position REPly	• Contains position of D. • Sent along the reverse path of the PDP.	LCA that finds D in its authentication table	Source node S

Table 5: Packets sent during route instantiation and maintenance phase of ARANz

Pid	Stand for	Description	From	To
RDP	Route Discovery Packet	• Sent to initiate route establishment to destination. • Sent using restricted directional flooding towards the destination node.	Source	Destination
RREP	Route REPly	• Initiated when the destination receives the first RDP. • Sent along the reverse path of the RDP.	Destination	Source
ERR	ERRor packet	• Generated if data is received on an inactive route or to report broken links in active routes. • All ERR packets must be signed. • Forwarded along the path toward the source without modification.	Node that notices the problem	Source

Table 6 Characteristics of the presented protocols [1]

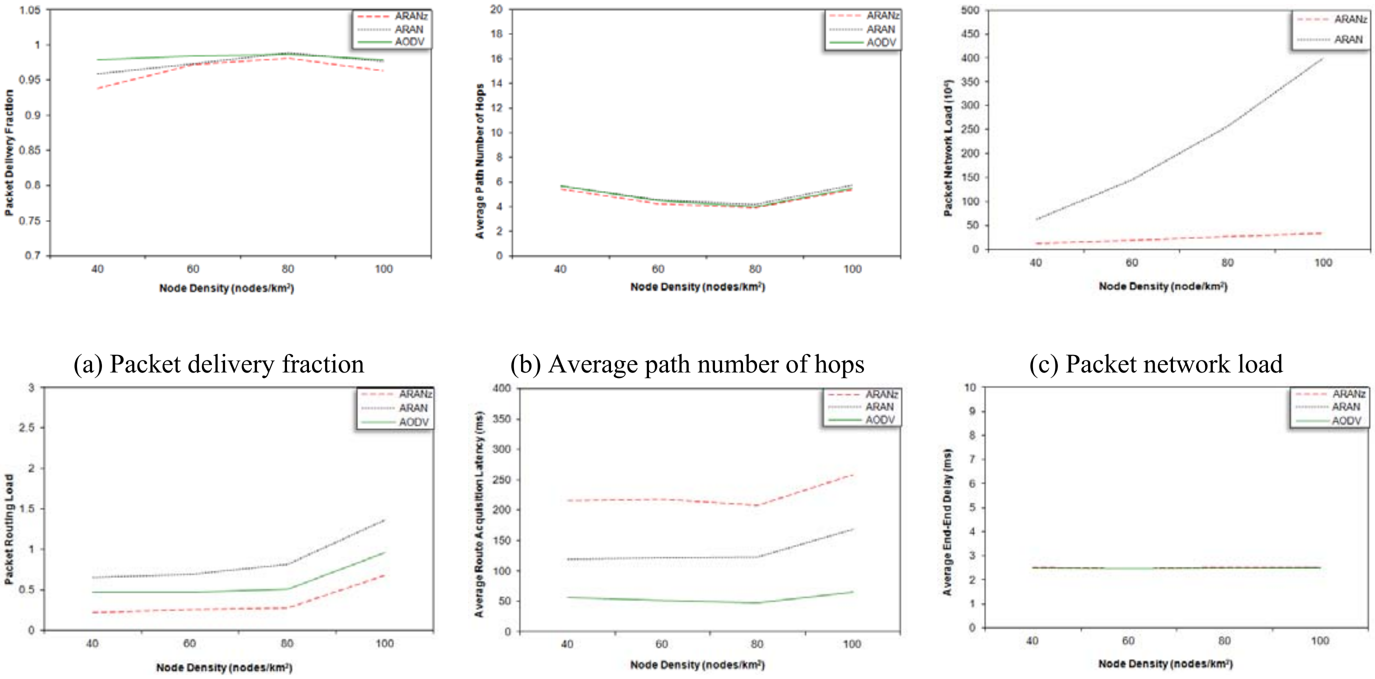
Performance parameter	**AODV**	**ARAN**	**ARANz**
Type	Topology-based (Reactive)	Topology-based (Reactive)	Position-based (Restricted Directional Flooding)
Secure	No	Yes	Yes
Route discovery sending mechanism	Route discovery packets are flooded to all nodes in the network.	Route discovery packets are flooded to all nodes in the network.	Intermediate nodes broadcast route discovery packet only if they are closer to the destination than the previous hop.
Main idea/ Contribution	Initiating a route discovery process only when the route is needed.	Protecting routing packets against attacks from malicious nodes in managed-open environments.	Solving scalability as well as single point of compromise and failure problems existing in ARAN protocol.
Proposal	Uses next hop information stored in the nodes of the route with the least number-of-hop field.	•Provides authentication of route discovery, setup and maintenance. •Uses cryptographic certificates to prevent most security attacks that face Ad-Hoc routing protocols. •Routing messages are authenticated at each hop from source to destination, as well as on the reverse path from destination to source.	•Divides area into zones and introduces multiple LCAs in each zone. •Requires sending a PDP if the position of the destination is unknown. •Uses restricted directional flooding to forward RDP. •Provides authentication of position update and discovery as well as route discovery, setup and maintenance. •Uses cryptographic certificates to prevent most security attacks that face Ad-Hoc routing protocols.
Path selection	Least number of hops	Quickest	Quickest
Loop freedom	Yes	Yes	Yes
Density	All	All	All
Load distribution	Yes	No	Yes
Centralized trust	No	Yes (Certificate Authority)	No (multiple LCAs in each zone)
Synchronization	No	No	Yes
Robustness	High	Low	Medium

Table 7: ARAN and ARANz security analysis [1]

Criterion	ARAN	ARANz
Secure extension of	AODV	AODV
Basic security mechanism	Certificates and timestamps	Certificates and timestamps
Central trust	Yes (CA)	No (multiple LCAs in each zone)
Availability	Low	Medium
Authentication	Yes	Yes
Confidentiality	No	Yes, if data is encrypted with destination public key
Integrity	Yes	Yes
Non-repudiation	Yes	Yes
Anonymity	No	No

Table 8: ARAN and ARANz robustness against existing attacks [1]

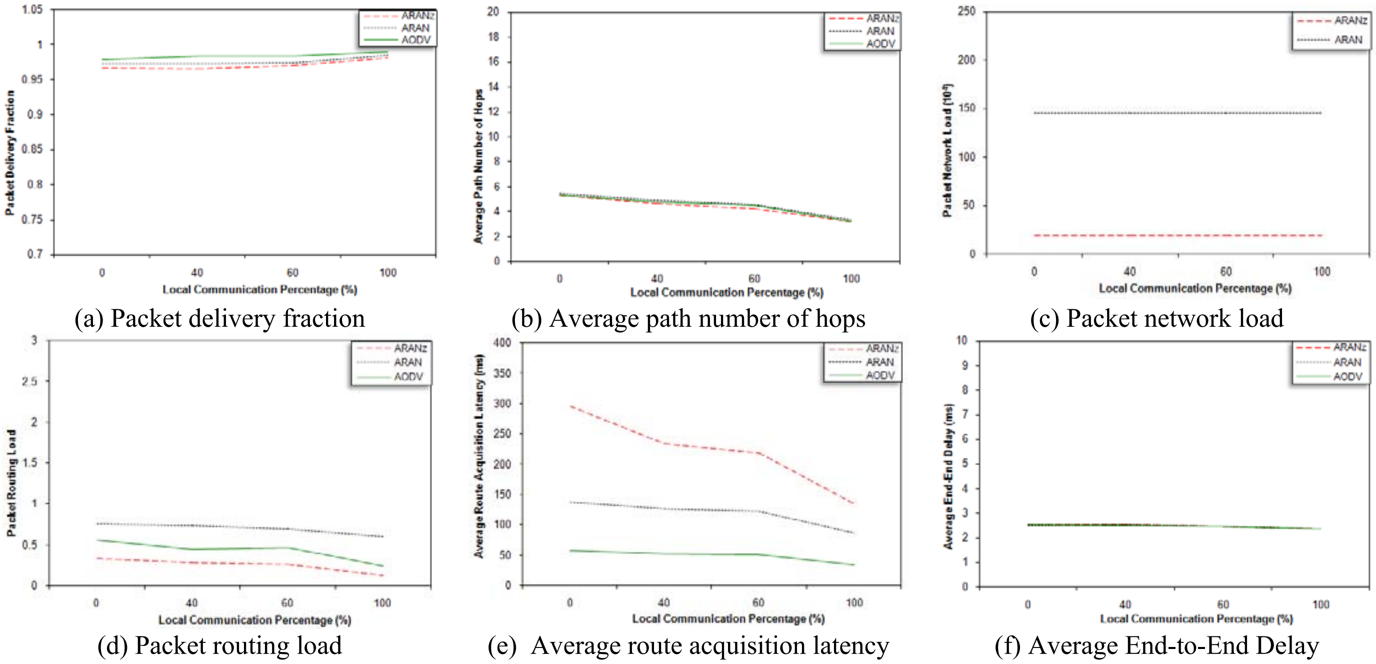
Type	Attack	Robust against
Passive attacks	Eavesdropping	Yes
Active attacks	Impersonation	Yes
	Fabrication	No, but provides non-repudiation
	Modification	Yes



(a) Packet delivery fraction (b) Average path number of hops (c) Packet network load

(d) Packet routing load (e) Average route acquisition latency (f) Average End-to-End Delay

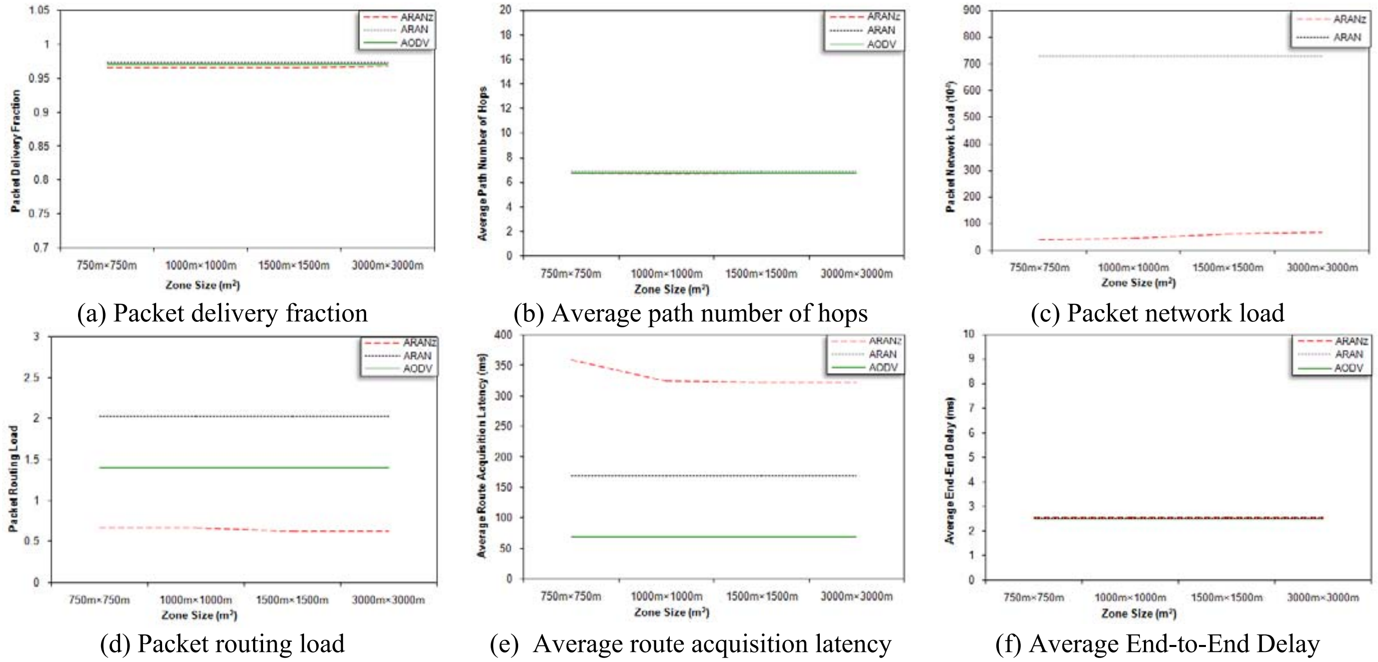
Figure 3 Node Density Effect



(a) Packet delivery fraction (b) Average path number of hops (c) Packet network load

(d) Packet routing load (e) Average route acquisition latency (f) Average End-to-End Delay

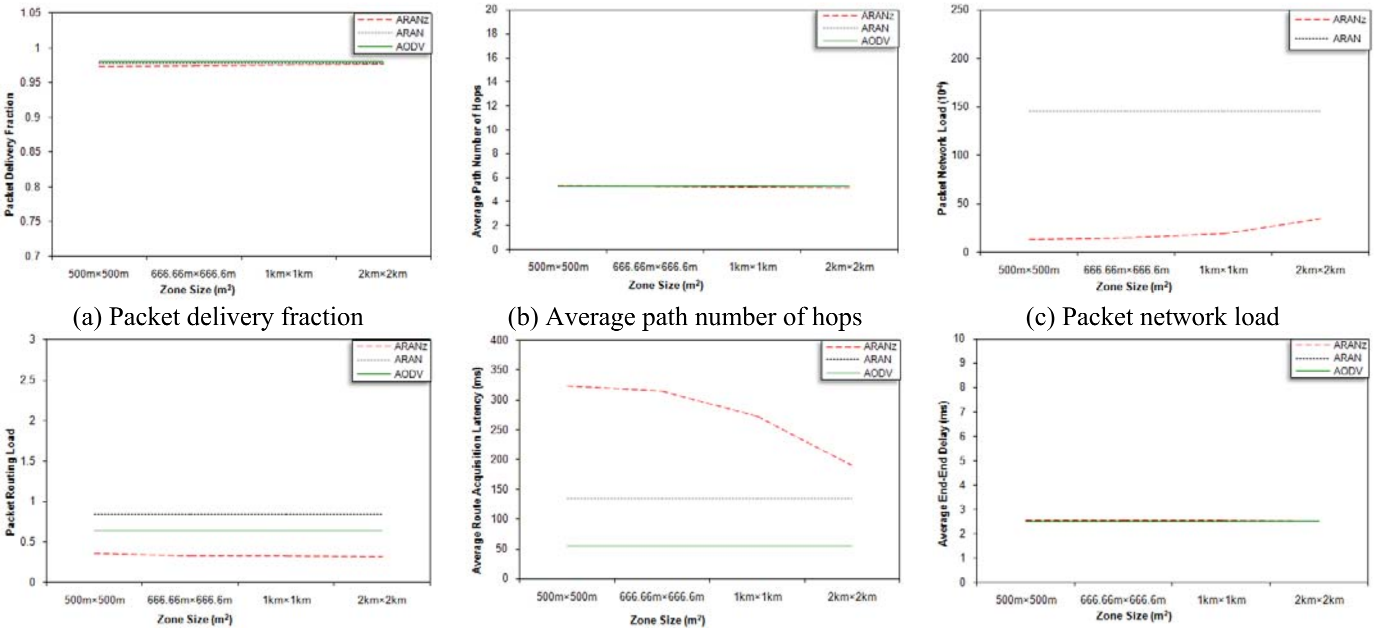
Figure 4 Local Communication Effect



(a) Packet delivery fraction (b) Average path number of hops (c) Packet network load

(d) Packet routing load (e) Average route acquisition latency (f) Average End-to-End Delay

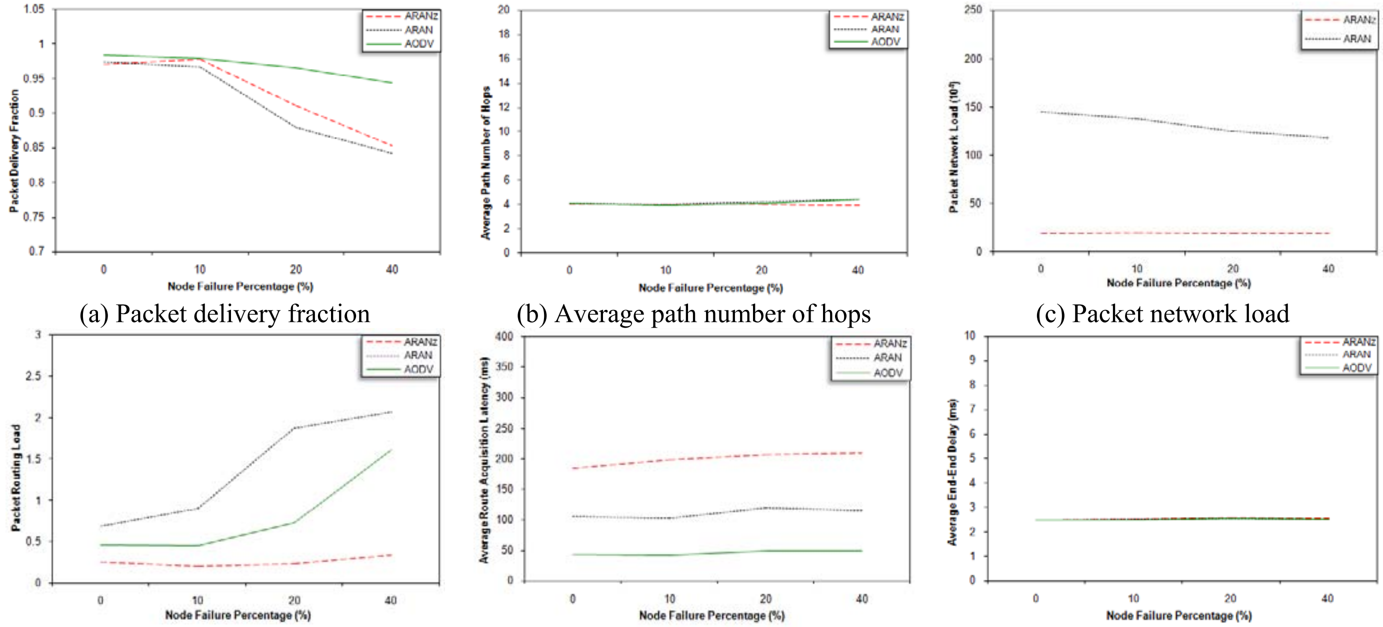
Figure 5 Zone Size Effect Considering 3km×3km Network



(a) Packet delivery fraction (b) Average path number of hops (c) Packet network load

(d) Packet routing load (e) Average route acquisition latency (f) Average End-to-End Delay

Figure 6 Zone Size Effect Considering 2km×2km Network



(a) Packet delivery fraction (b) Average path number of hops (c) Packet network load

(d) Packet routing load (e) Average route acquisition latency (f) Average End-to-End Delay

Figure 7 Node Failure Percentage Effect