ASTES

*Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 5, 176-192 (2020)*

www.astesj.com

**ASTESJ**

**ISSN: 2415-6698**

# Detailed Security Evaluation of ARANz, ARAN and AODV Protocols

Liana Khamis Qabajeh[1, *], Mohammad Moustafa Qabajeh[2]

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

[2]*Faculty of Information Technology and Computer Engineering, Palestine Technical University Kadorie, Palestine*

ARTICLE INFO

*Article history:*
*Received: 12 May, 2020*
*Accepted: 02 September, 2020*
*Online: 10 September, 2020*

*Keywords:*
*Position-based*
*Secure*
*Scalable*
*Routing protocol*
*Location service*
*Mobile Ad-Hoc networks*
*Security evaluation*
*ARANz*
*ARAN*
*AODV*

ABSTRACT

*Ad-Hoc networks are self-organized wireless networks. Finding a secure and efficient route leading from a specific source node to an intended destination node is one of the serious concerns in mobile Ad-Hoc networks. ARANz is one of the significant protocols that has been proposed for such networks. ARANz implements the authentication methods used with the original Authenticated Routing for Ad-Hoc Networks (ARAN) and enhance security and attain robustness by dividing the network into zones and introducing several local certificate authority servers. Using restricted directional flooding, ARANz reveals improved scalability and performance.*

*The purpose of this paper is to discuss in details the misbehavior detection system used with ARANz protocol, along with presenting a detailed simulated security and performance evaluation of ARANz and other existing protocols. Through extensive simulation using GloMoSim simulator, a detailed security evaluation has been conducted to evaluate ARANz and compare it with the original ARAN and Ad-Hoc On-demand Distance Vector (AODV). Simulation results confirm the effectiveness of ARANz in discovering secure routes within quite large networks including large number of moving nodes, while retaining the minimum packet routing load. Results also prove that ARANz has superior performance regardless malicious nodes percentage conducting different types of attacks such as modification, black hole, grey hole and fabrication. Hence, ARANz can be a good choice for Ad-Hoc networks established among students on a campus or peers at a conference, where pre-deployment of some keys and certificates is possible.*

## 1. Introduction

Ad-Hoc networks are self-configurable and self-organized networks without centralized control. Unstable infrastructure, scarcity of resources and dynamic network topology are some Ad-Hoc networks properties that made efficient routing one of the important issues especially that routing is conducted in a multi-hop fashion and all nodes act as both hosts and routers. In addition, the concept and nature of Ad-Hoc networks result in making them exposed to attacks using modification, impersonation and fabrication [1], [2]. Hence, safe exchanging of data through the network has been a challenging task.

Managed-open environment might be found among students on a campus or peers at a conference. In such environments, there is an opportunity of using previously established infrastructure and pre-deployment of some keys and certificates [1], [2]. However, the approach that depends on a single centralized server is unfeasible for Ad-Hoc networks, as it might be the operation bottleneck [1]. Hence, the certificate authority and position service are supposed to be distributed among numerous servers. Moreover, the demand for scalable and energy-efficient routing protocols, along with the availability of small and low power positioning devices lead to adopting position-based routing in mobile Ad-Hoc networks.

A new distributed and secure position-based routing protocol, ARANz, has been proposed in our work in [1]. Adopting the original Authenticated Routing for Ad-Hoc Networks (ARAN) [2], ARANz seeks to enhance the routing protocol performance and distribute the routing load by dealing with the network as zones. Additionally, it looks for achieving robustness, enhancing security, solving the single point of failure and avoiding single point of attack via distributing trust among multiple certificate authority

*Corresponding Author: Liana Khamis Qabajeh, liana_tamimi@PPU.EDU

servers. Finally, ARANz utilizes restricted directional flooding to exhibit enhanced scalability, robustness and performance.

This paper is an expansion of our work in [1]. A detailed discussion of the ARANz protocol, security analysis of ARAN and ARANz protocols, along with simulated performance evaluation among Ad-Hoc On-demand Distance Vector (AODV) [3], ARAN and ARANz protocols have been conducted in [1]. This work, on the other hand, presents a detailed discussion of the Misbehavior Detection System used with ARANz protocol. Moreover, this paper presents a detailed simulated security and performance evaluation of AODV, ARAN and ARANz protocols. This paper also evaluates the effectiveness of these protocols in tackling security concerns considering different number of malicious nodes found in the network and perform diverse attacks such as modification, black hole, grey hole and fabrication. Hence, in this research, we propose a novel Misbehavior Detection System, integrate it with the ARANz protocol, and conduct detailed simulated security and performance evaluation of AODV, ARAN and ARANz protocols.

Through this research we are trying to answer the following research question; will identifying and isolating the malicious nodes in ARANz help in achieving high level of performance and security compared to the other two protocols? Hence, we can set out and try to prove our research hypotheses; that is, utilizing the proposed misbehavior detection system with ARANz will improve its performance and security.

Results prove that ARANz is able to find out secure routes effectively and is still able to have superior performance even with having large percentage of malicious nodes conducting different types of attacks. Moreover, ARANz maintained the minimum packet routing load in all conducted scenarios compared to AODV and ARAN protocols, which assures its scalability. The price of ARANz is a longer latency in route discovery due to the required time for authentication, packet processing together with obtaining the position of the destination.

The rest of the paper is structured as follows. Section 2 discusses Ad-Hoc networks routing protocols security and introduces AODV and ARAN protocols. Section 3 presents ARANz protocol including a detailed discussion of the proposed misbehavior detection system. Section 4 provides security analysis along with a simulated comparison among AODV, ARAN and ARANz protocols. Our findings are discussed in Section 5 and our work is concluded in Section 6. To conclude, future directions are presented in Section 7.

## 2. Background and Related Work

This section presents security issues and conducted efforts to ensure security in Ad-Hoc networks. Subsection 2.1 discusses Ad-Hoc routing protocols security issues; including different security requirements along with some attacks conducted to disrupt an Ad-Hoc network security. Subsection 2.2 discusses recent conducted efforts related to Ad-Hoc networks security. While, Subsections 2.3 and 2.4 introduce AODV and ARAN protocols since our protocol will be compared to them.

### *2.1. Ad-Hoc Routing Protocols Security*

Ensuring Ad-Hoc network security requires satisfying many requirements [4]-[8]. One important requirement is confidentiality. *Confidentiality* ensures that sensitive data being sent through the network are kept secret; i.e., messages content may be interpreted merely by their source and destination. Another requirement is *integrity* which assures that a message sent over the network is not corrupted whether intentionally or accidentally. *Availability* means that network should stay operational and accessible to allow sending and receiving messages at any time. Additionally, the nodes identities assure that they are who they pretend to be; *authentication*. *Non-repudiation* assures that neither sender nor receiver should be able to deny sending or receiving a message. Moreover, *privacy* has become a key security issue and numerous efforts considering anonymous Ad-Hoc routing protocol have been proposed. The *anonymity* in an Ad-Hoc network assures that the identity of nodes, route paths information and location information must be unidentified not only by adversary nodes but also by other nodes in the network.

Routing is an essential operation in Ad-Hoc networks; so, it is a major target for attackers to disrupt an Ad-Hoc network. Many attacks [5], [9], [10] may be performed against Ad-Hoc networks. *Fabrication* attack is carried out by generating deceptive routing packets. These attacks are hard to be recognized as they appear as legitimate routing messages. *Modification* attack targets the routing computation integrity. By altering routing information, an attacker may result in network traffic dropping, or redirecting to another destination, or taking a longer path to the destination. In *Impersonation* attack, a malicious node may conduct various attacks and fake the network topology by pretending to be another legitimate node.

### *2.2. Recent Works in Ad-Hoc Networks Security*

Recently, many research efforts have been conducted considering Ad-Hoc networks security. Some of them, such as [11]-[14], have discussed and elaborated a comprehensive analysis of Ad-Hoc networks security issues due to its special characteristics along with presenting the proposed defeating approaches against existing attacks.

Some other researchers conducted security assessment and evaluation of existing Ad-Hoc networks secure routing protocols. Authors in [15], for example, examined the performance of AODV routing protocol under numerous security attacks. They found that conducting diverse attacks results in lower throughput and packet delivery ratio. Additionally, authors in [16], studied the performance and security of AODV routing protocol and Secure Ad hoc On demand Distance Vector routing protocol [17] taking into account various attack types including replay and blackhole attacks.

Other researches proposed new security solutions to avoid specified Ad-Hoc networks attacks. In [18] and [19] new flooding attacks prevention routing protocols have been proposed. In [20] a triple factor architecture of a secured scheme has been suggested for environments considering reactive routing protocols such AODV. In this architecture, each node computes the trust considering the direct information then verifies the reputation via gathering information from its neighboring nodes and uses a cryptographic algorithm to ensure security. Integrating the proposed procedure at every node enhances the throughput and lowers the overhead even upon malicious nodes existence.

Authors in [2] proposed ARAN protocol to prevent a number of attacks such as modification, impersonation and fabrication exploits. In [21], authors proposed a quantitative trust model for Ad-Hoc networks those are integrated with Internet of Things (IoT). The proposed model combines both direct and indirect trust to calculate a node's final trust value. Diverse trust evidences along with direct trust have been taken into account. Moreover, only trusted nodes are chosen in the route between source and destination to ensure secure and reliable packets delivery. Detailed discussions of recent research work done on security solutions for Ad-Hoc networks can be found in [11]-[13], [22].

One protocol of interest is the ARAN protocol since it provides authentication of route discovery, setup and maintenance as well as message integrity and non-repudiation. Moreover, ARAN prevents a number of attacks such as modification, impersonation and fabrication exploits. ARAN is a secure extension of AODV. One advantage of reactive routing protocols, such as AODV, is that no periodic routing packets are required. In the following two subsections, AODV and ARAN protocols are further explained since our protocol has been proposed based on and will be compared to them.

### *2.3. Ad-Hoc On-demand Distance Vector (AODV)*

Ad-Hoc On-demand Distance Vector (AODV) [3] is a reactive routing protocol, i.e. it uses flooding to detect routes on-demand. The query packet in AODV has a number-of-hop field which is incremented by all intermediate nodes. AODV forwards data packets based on next hop information maintained on the nodes involved in the route. Reactive routing protocols have the advantage that there is no need for periodic routing packets. On the other hand, they may have increased control overhead in high mobility and heavy traffic loads environments. Scalability is considered to be another weakness since they rely on blind broadcast to find routes. Broadcasting routing packets to the entire network leads to congestion and large routing overhead along with affecting the protocol's performance due to dropping data packets.

### *2.4. Authenticated Routing for Ad-Hoc Networks (ARAN)*

Authenticated Routing for Ad-Hoc Networks (ARAN) [2] is similar to AODV, but provides authentication during different phases. The main intention of ARAN is to protect routing packets against attacks conducted by malicious nodes in a managed-open environment. Hence, it requires some security coordination before deployment. It assumes the existence of a trusted Certificate Authority (CA) server. All trusted nodes are aware of the public key of the CA. Each node requests a certificate from this CA before joining the Ad-Hoc network. ARAN uses cryptographic certificates to avoid most security attacks targeting Ad-Hoc routing protocols, including message integrity, authentication and non-repudiation.

ARAN consists of a preliminary certification step followed by a route discovery process. In a try to find a route in ARAN, source node broadcasts a Route Discovery Packet (RDP), which is responded to by a unicast REPly (REP) packet that is initiated by the intended destination, and forwarded along the reverse path towards the source. Routing packets are end-to-end authenticated and only authorized nodes participate in sending these packets. Consequently, each node that forwards a request or a reply signs it to enable the subsequent node to check the validity of the previous one.

Compared to original AODV, ARAN prevents numerous attacks including altering routing messages, misrepresenting node's identity (spoofing attack) and injecting into the network routing messages that have been previously captured (replay attack). Furthermore, simulations in [2] show that ARAN performance is equivalent to that of AODV in discovering and maintaining routes.

In contrast, in addition to scalability problem with the number of nodes (which is inherited from AODV) ARAN incurs additional packet overhead and longer route discovery latency due to signing each packet. Lastly, ARAN uses single certificate server which results in a need to keep it uncompromised. Depending on a centralized certificate authority in a physically insecure environment forms a single point of capture and compromise reducing protocol's availability and robustness against attacks.

## 3. ARANz Routing Protocol

In this section, our proposed protocol along with the proposed misbehavior detection system are presented. Section 3.1 shows our methodology and assumptions. Section 3.2 gives a basic presentation of ARANz phases, while Section 3.3 tackles a detailed discussion of the proposed misbehavior detection system.

### *3.1. Methodology and Assumptions*

ARANz routing protocol [1] adopts ARAN protocol authentication steps along with dividing the network into virtual zones. In ARANz, cryptographic certificates are used to avoid most of the attacks threaten Ad-Hoc routing protocols and to discover irregular behavior. However, ARANz suggests a hierarchal routing model, aiming to improve routing protocol performance and share out load via dealing with the area as zones. Furthermore, ARANz aims to attain high level of security and robustness, solve the single point of failure and attack problems by distributing trust among several Local Certificate Authority (LCA) servers. Every zone has numerous LCAs collaborating together to issue certificates for the nodes residing currently within this zone.

Furthermore, ARANz tries to demonstrate improved scalability, performance and robustness against regular topological changes through applying restricted directional flooding concept. So, LCAs also play the role of position servers and nodes contact LCAs of their zones informing them about their new position upon movement. ARANz also proposed a misbehavior detection scheme to improve its security. Within this scheme, the procedure to identify misbehaving nodes, and the needed actions to be taken upon discovering them are proposed to mitigate service interruption.

ARANz assumes that nodes are arbitrarily distributed in a square-shape area and know their positions. Primary Certificate Authority (PCA) is a pre-chosen node having the required software to divide the area into zones and elect the preliminary LCAs. PCA possesses the network private key ($K_{NET-}$). All trusted participating nodes own a private/public key pair and the network public key ($K_{NET+}$).

### *3.2. ARANz Phases*

ARANz consists of five phases. These phases are network setup, network maintenance, location service, route instantiation

and maintenance and lastly data transmission. PCA initiates *Network setup phase*, divides the area into zones and elects the initial LCAs. *Network maintenance phase* ensures preserving the network hierarchy considering some concerns including nodes certificates update, LCAs synchronization, nodes movements along with destroyed and corrupted nodes. Figure1 shows the network structure supposing that the entire area is divided into sixteen zones.

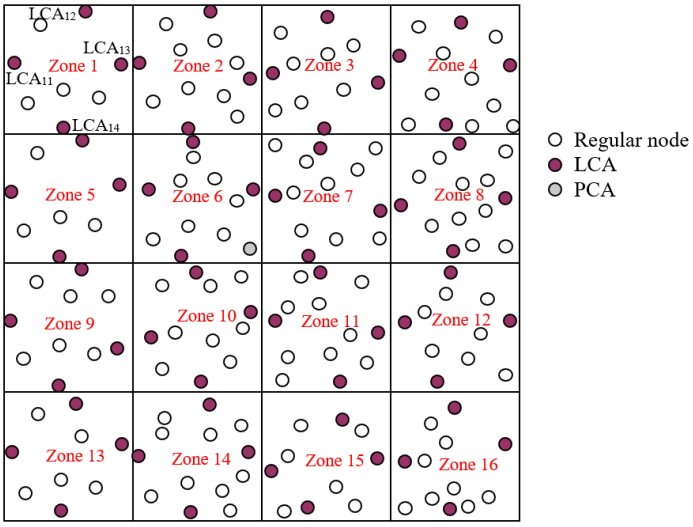



Figure 1: Network structure after electing initial LCAs

When a source has data to send to a specific destination; source should obtain the position of the destination before conducting the route discovery procedure. *Location service phase* allows the source to acquire the position of the destination via Position Discovery Packets (PDP) and Position REPly (PREP) packets.

After obtaining the destination position, *route instantiation and maintenance phase* is started using Route Discovery Packets (RDP), Route REPly (RREP) packets and ERRor (ERR) packets. After accomplishing route discovery and setup, the source starts *data transmission phase* and sends data to the intended destination via the selected route.

Table 1 summarizes the different phases in ARANz protocol. A detailed discussion of ARANz different phases, along with the packets sent during each phase can be found in our work in [1]. In the following subsection we concentrate on the details of the suggested Misbehavior system considering malicious nodes residing in the network and conducting different attacks such as modification, black hole, grey hole, and fabrication.

Table 1: ARANz protocol different phases

| Phase | Explanation |
|---|---|
| Network setup | Consists of issuing certification, dividing network into zones, deciding on initial LCAs and informing each node about the initial role it will play in the network. |
| Network maintenance | Ensures maintenance of the network structure, considering updating nodes certificates, needed synchronization, as well as nodes movement, corrupting and distortion. |
| Location service | Allows source to obtain position of the destination by communications with its zone LCAs. |
| Route instantiation and maintenance | Includes sending a RDP via restricted directional flooding from source to destination, unicasting a RREP from the destination along the reverse path towards the source and maintaining the selected route using ERR packets to announce broken links in active paths. |
| Data transmission | Relaying data packets through the selected route during the route instantiation process until reaching the destination. |
| Misbehavior detection system | Helps in identifying malicious nodes and excluding them from future communications. |

Let us define some notations and variables to be used in the forthcoming sections. Table 2 presents variables, notations and packet identifiers used with ARANz protocol. While, Table 3 shows the notation used to present the suggested misbehavior detection system.

Table 2: Variables, notations and packet identifiers for ARANz

| Notation | Explanation | Notation | Explanation |
|---|---|---|---|
| PCA | Primary Certificate Authority | $LCA_{zs}$ | Zone *z* Local Certificate Authority *s* |
| $LCAsZ_z$ | Zone *z* LCAs identities and positions | $IP_n$ | Node *n* IP address |
| $N_n$ | Node *n* Nonce | $Cert_n$ | Node *n* Certificate |
| $K_{n-}$ | Node *n* Private key | $K_{n+}$ | Node *n* Public key |
| $K_{NET-}$ | Network Private key | $K_{NET+}$ | Network Public key |
| $\underrightarrow{Rdf}$ | Send packet using restricted directional flooding | $\underrightarrow{Fln}$ | Flood packet to entire network |
| MNODE | Misbehaving NODE | CNODE | Compromised NODE |
| PDP | Position Discovery Packet | RDP | Route Discovery Packet |
| PREP | Position REPly packet | RREP | Route REPly packet |
| ERR | ERRor packet | | |

Table 3: Variables and notations for the proposed misbehavior detection system

| Notation | Explanation | Notation | Explanation |
|---|---|---|---|
| $Fd_{nm}$ | Number of dropped data packets by node m that it receives from node n | $Fm_{nm}$ | Number of modified control packets sent from node m to node n |
| Nm | Number of packets received indicating the misbehavior of a node so that this node is considered as compromised | $Sd_{nm}$ | Number of delivered data packets by node m that it receives from node n |
| $Sm_{nm}$ | Number of unmodified control packets sent from node m to node n | $TrstVd_{nm}$ | Node n trust value regarding node m considering dropping attacks |
| $TrstVf_{nm}$ | Node n trust value regarding node m considering fabrication attacks | $TrstVm_{nm}$ | Node n trust value regarding node m considering modification attacks |
| Thd | Dropping threshold | Thf | Fabrication threshold |
| Thm | Modification threshold | TT | Trust table |

### *3.3. Misbehavior Detection System*

Malicious nodes might conduct erratic actions such as using invalid certificates and inappropriately signed massages. ARANz responds to all erratic behaviors by dropping any packet showing any erratic behavior.

Malicious nodes, however, may cause more severe misbehaving actions and attacks, such as altering some fields in control packets, dropping data packets and fabricating error packets. In these cases, our protocol collaborates with a misbehavior detection system to help in detecting and isolating malicious nodes, such as the one proposed in this section.

The proposed system is powerful regarding flexibility and accuracy in managing trust and lightweight in terms of computation. Our system is flexible and can be used to protect against several attacks. The main concept is that each node has a trust table (TT) to maintain reputation information regarding neighboring nodes. In the TT, values about several events are stored. A node uses this value to evaluate its neighbor as misbehaving (malicious) or well-behaving node. Each node is responsible for gathering events from direct relations and computing its own trust values for its neighbors.

Section 3.3.1 discusses the process of collecting data about different trust metrics. After that, dealing with malicious and compromised nodes are explained in Sections 3.3.2 and 3.3.3, respectively.

#### *3.3.1 Data Collection and Trust Metrics Calculation*

Whenever a misbehaving action is detected, it triggers a response by the neighboring nodes. Hence, one important aspect of trust management systems is collecting data. Consequently, it is necessary to identify what events reflect a helpful feedback to the scheme and assist in making the proper decision.

Many trust metrics can be considered to disclose the cooperation willingness of nodes during route establishment and maintenance as well as data forwarding phases, however, as trade-off between implementation cost and intended security, a number of these metrics have been selected in this work. The behavior aspects that have been chosen for monitoring are:

- Control packet modification: nodes assemble trust information regarding their neighbors during interactions considering the try to modify some fields in PDP, PREP, RDP or RREP packets.
- Data packet dropping: nodes are evaluated concerning their sincerity and willingness in forwarding data packets, trying to reduce grey-hole and black-hole attacks. Readiness can be checked either based on link layer acknowledgements, or through overhearing [23].
- Error packet fabrication: to protect against fabricating ERR packets, each node keeps information about the number of ERR packets issued by each neighbor.

Let us now quantify these aspects. For the first two trust metrics, node A calculates trust values concerning node B considering modification attacks ($TrstVm_{AB}$) and dropping attacks ($TrstVd_{AB}$) using (1) and (2).

$$TrstVm_{AB} = \frac{Sm_{AB}}{Sm_{AB} + Fm_{AB}} \quad (1)$$

$$TrstVd_{AB} = \frac{Sd_{AB}}{Sd_{AB} + Fd_{AB}} \quad (2)$$

Where $Sm_{AB}$ and $Sd_{AB}$ consider the number of successful co-operations, whereas $Fm_{AB}$ and $Fd_{AB}$ consider the number of failed ones. In other words, for the first metric $Sm_{AB}$ is the number of unmodified control packets and $Fm_{AB}$ stands for the number of modified control packets received by node A from node B. For the second metric, $Sd_{AB}$ stands for the number of delivered data packets and $Fd_{AB}$ is the number of dropped data packets by node B that it already received from node A.

For the last trust metric, node A computes a trust value concerning neighbor B considering ERR packets fabrication attack ($TrstVf_{AB}$) by counting the ERR packets issued by B that passes through node A towards the source.

#### *3.3.2 Malicious Nodes*

Once $TrstVm_{AB}$ or $TrstVd_{AB}$ become less than a threshold Thm or Thd respectively, node A considers node B as a malicious node. Also, if $TrstVf_{AB}$ becomes higher than a threshold Thf, node A believes that node B is a malicious node. In these cases, node A excludes node B from upcoming communications. Moreover, node A sends a Misbehaving NODE (MNODE) packet to announce this misbehavior to its nearest zone LCA. This packet

is sent via Restricted directional flooding (Rdf). Suppose that the nearest LCA to node A is node I, then node A sends the following MNODE packet to node I:

$$A \xrightarrow{Rdf} I: [MNODE, IP_I, N_A, IP_B] K_{A-}, Cert_A$$

The MNODE packet contains a packet type identifier (MNODE), the nearest LCA IP address ($IP_I$), the sending node nonce ($N_A$) and the misbehaving node IP address ($IP_B$). The principle of the nonce is to distinctively identify a MNODE packet sent by a specific node. Every time A sends a MNODE packet, it adds up the nonce value. The packet is signed by the node private key ($K_{A-}$) and node certificate ($Cert_A$) is added to the packet to allow other nodes to authenticate the signature and ensure that A certificate is still active.

*3.3.3 Compromised Nodes*

From the reputation of a node, it can be identified as misbehaving, consequently, it may be eliminated from the routing process if it is proved to be a misbehaving node. In our scheme, if major part of LCAs in a specific zone have collected a pre-defined number (Nm) of MNODE packets indicating the misbehavior of a particular node, then they work together and send a Compromised NODE (CNODE) message to the entire network. Consequently, this node is excluded by other nodes until its certificate expires normally. Suppose that the nearest LCA to the compromised node is node I, then node I will broadcast the following CNODE packet:

$$I \xrightarrow{Fln} ALL: [CNODE, N_I, [IP_B] K_{NET-}] K_{I-}, Cert_I$$

The CNODE packet is sent using network flooding (Fln) technique. In network flooding, a packet is forwarded to all nodes existing currently in the network. Thus, each node upon receiving a packet continues broadcasting the packet to all its neighbors. The CNODE packet contains a packet type identifier (CNODE), the nonce of the sending node ($N_I$) and the IP address of the compromised node ($IP_B$). CNODE packets are signed by the private key of the node ($K_{I-}$) and node certificate ($Cert_I$) is appended to the packets to enable other nodes to validate signature and verify certificate freshness. To ensure that the node initiated the packet is truly one of the trusted LCAs, the compromised node IP address is signed by $K_{NET-}$.

Same procedure is appropriate if the misbehaving node is a LCA. Thus, if three LCAs of a specific zone received a pre-defined number of MNODE packets demonstrating the misbehavior of the fourth LCA, this LCA is taken out from the LCAs list ($LCAsZ_z$) of this zone, a CNODE packet is broadcast and a new LCA election procedure is initiated. Even before withdrawing the certificate from the misbehaving LCA, other LCAs can give certificates for trusted nodes in this zone even if the compromised LCA refused to initiate ACREP packets.

If two LCAs of the same zone are compromised simultaneously, neither the two compromised LCAs nor the trusted LCAs are able to issue certificates. This state may stay till the expiration of certificates of zone nodes. Accordingly, these nodes become unable to take part of any upcoming activity. This state may also end (before the expiration of nodes' certificates) by losing battery energy of one compromised LCA or its departure to a neighboring zone. At this point, a new LCA election is conducted to substitute the compromised LCA. Having a third well-behaving LCA, these LCAs can perform their tasks normally.

On the other hand, this state may end by replacing a trusted LCA with a compromised one (e.g. the trusted LCA moved to a neighboring zone and the newly elected LCA is compromised). Now, there are three compromised LCAs in this zone. Hence, the security of the entire network is compromised and these LCAs may work together to give certificates to misbehaving nodes.

*3.3.4 Misbehavior Detection System Summary*

This section has discussed the misbehavior detection system in details. Table 4 summarizes the packets sent during the misbehavior detection system phase.

Table 4: Packets sent during the misbehavior detection phase of ARANz

| Pid | Stand for | Explanation |
|---|---|---|
| MNODE | Misbehaving NODE | • Sent to report the misbehavior of other nodes.<br>• Sent using restricted directional flooding.<br>• Sent from any regular node n to nearest LCA in its zone z. |
| CNODE | Compromised NODE | • Sent after collaboration of the majority of LCAs in zone z upon receiving the pre-defined number of MNODE packets for a specific misbehaving node.<br>• Sent using network flooding.<br>• Sent from LCAs of zone z to All nodes |

## 4. Performance and Security Evaluation

Our next step is to study ARANz performance and security and compare it with existing protocols. Section 4.1 shows our simulation environment and methodology. Section 4.2 through Section 4.6 study the effect of the malicious node percentage conducting modification, black hole, grey hole, fabrication and multiple attacks, respectively.

*4.1. Simulation Environment and Methodology*

Our protocol should be compared with the basic ARAN protocol since our protocol is based on it. Additionally, AODV protocol is also considered since AODV is usually considered as a benchmark for Ad-Hoc routing protocols performance evaluation and as ARAN is proposed based on AODV. In the following subsections a detailed simulated performance and security evaluation of the three routing protocols is provided.

Evaluating the performance of AODV, ARAN and ARANz protocols is conducted using GloMoSim simulation tool. Nodes transmission range of 250m is simulated. The nodes initial positions are randomly chosen with node density of 60nodes/$km^2$. After that, nodes may travel regarding the random waypoint mobility model, i.e., every node moves to a randomly selected position at a specified speed and then pauses for a chosen pause time, before selecting another random position and repeating these steps.

Source and destination pairs are randomly chosen for both local and external communications. 802.11 MAC layer and Constant Bit Rate (CBR) traffic over User Datagram Protocol (UDP) are used. Five CBR sessions are conducted in all runs. Each session generates 1000 512-byte data packets at the rate of 4 packets per second. A percentage of 60% of local communication is considered, i.e., two of the five CBR sessions in each run are external and the others are local.

For simulating ARAN and ARANz, it has been assumed that the key distribution procedure has been completed. A 512-bit key and 16-byte signature are simulated [2].

For either protocol, a routing packet processing time of 1ms is simulated [3]. Moreover, a processing delay of 2.2 ms is added for the ARAN and ARANz cryptographic operations [2]. In order to minimize collisions, an arbitrary delay between 0 and 10ms is added before forwarding a broadcast packet.

The effect of malicious node percentage has been tested considering the following *performance metrics*:

1. Packet Delivery Fraction (PDF): fraction of the generated data packets by the source nodes that are received by intended destination nodes.
2. Average Path Number of Hops (APNH): average length of the discovered routes by a protocol. It is evaluated by averaging the number of hops needed by different data packets to arrive at their destinations.
3. Packet Network Load (PNL): resulted overhead packets to construct and maintain network structure along with updating certificates and positions of nodes. It is evaluated in ARANz as the total of all packets sent throughout the setup and maintenance phases. Alternatively, it is calculated in ARAN as the summation of transmitted packets to certify nodes. The forwarding at every hop along the routes is also considered in this metric calculation. Regarding AODV, it is an unsecure flat topology-based protocol; i.e., it has no network structure maintenance nor nodes positions or certificates update. Hence, PNL of AODV is not included in the figures.
4. Packet Routing Load (PRL): ratio of routing packets to delivered data packets. Routing packets include all packets sent throughout the location service, route instantiation and route maintenance phases. Retransmission at all hops along the path is also considered.
5. Average Route Acquisition Latency (ARAL): average time to discover a route to the destination. It is calculated in ARAN and AODV as the average delay from sending a route discovery packet by a source to receiving the first related route reply packet. Considering ARANz, it is calculated as the average time needed for both discovering the destination position and finding a route to it.

Each point in the following figures is an average of five simulation runs with similar configuration but different randomly generated numbers. Several scenarios have been conducted for numerous attacks with different number of attacking nodes. The effect of malicious nodes behavior is studied on a 2km×2km network containing 240 nodes and is divided into 4 zones. These nodes move at a maximum speed of 5m/s. Simulations are run with randomly chosen 0%, 10%, 20% and 40% malicious nodes.

To investigate the malicious node percentage effect, five scenarios have been simulated. Malicious nodes perform the following attacks towards data and/or control packets:

1. Modification attack: Malicious nodes performing modification attack selectively reset the hop count field to 0 in the route discovery and setup packets passing through them. By assigning the hop count field to 0, a malicious node makes other nodes believe that it is just one hop from the source or destination.
2. Black hole attack: Misbehaving nodes dump every data packet that they are supposed to forward.
3. Grey hole attack: Misbehaving nodes drop some data packets at random intervals.
4. Fabrication attack: Misbehaving nodes performing this attack periodically fabricate error packets with a specific probability.
5. Multi-attack: Malicious nodes carry out multiple attacks with a specific probability.

For these scenarios some or all the following *security metrics* have been added, as necessary, to the set of the studied performance metrics:

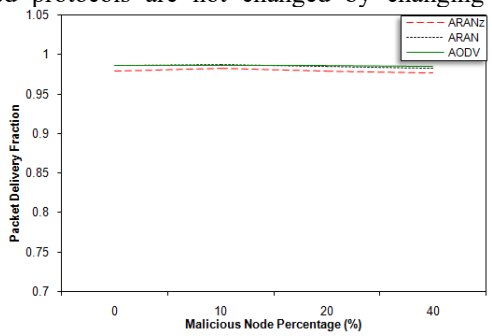
1. Malicious Route Percentage (MRP): portion of the selected routes that pass through malicious nodes. It is evaluated as the number of routes having misbehaving nodes within them over the number of all used routes.
2. Packet Loss Percentage (PLP): fraction of data packets that are abandoned by malicious nodes without any notification.
3. Fabricated Error Packets (FEP): number of error packets that are fabricated by misbehaving nodes.
4. Compromised Node Percentage (CNP): fraction of nodes that are treated as compromised due to recognizing their misbehavior.
5. Packet Malicious Load (PML): extra packets sent for the misbehavior detection system including MNODE and CNODE packets. The transmission at each hop is also considered in this metric calculation.

The last two metrics are only specified for ARANz since the other two protocols do not have misbehavior detection schemes. Some initial experiments have been carried out to choose the best values for modification threshold (Thm), dropping threshold (Thd), fabrication threshold (Thf) and the number of MNODE packets that LCAs should receive to consider a specific node as compromised (Nm). Different values for Nm are considered ranging from 1 to 3, also Thm and Thd are assigned values ranging from 0.3 to 0.7. Finally values of Thf range from 3 to 7. Results of these experiments show that a larger number of misbehaving nodes are really identified as compromised nodes upon setting Nm, Thm, Thd and Thf to 1, 0.5, 0.5 and 3, respectively. Accordingly, these are the values that are assigned for these parameters upon simulating different scenarios.

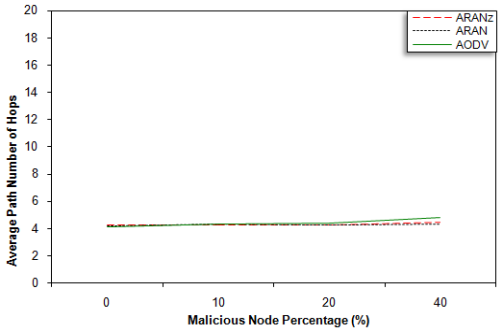
### 4.2. Malicious Node Percentage Effect Considering Modification Attack

In this scenario, the simulated malicious behavior represents the modification attack. Upon receiving a route discovery or reply, a malicious node chooses a random number between 0 and 1. If the chosen number is lower than 0.5, then the node illegitimately assigns the value of 0 to the hop count field, to convince other nodes that it is only one hop from the source or destination. If not, it forwards the control packet without modification.

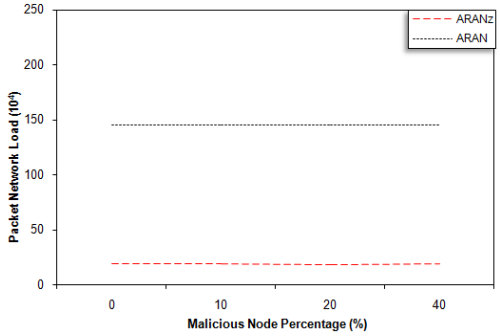
It is clear from Figure 2 (a through e) that the first five metrics of the three studied protocols are not changed by changing malicious node percentage, except APNH and ARAL for AODV. This fact indicates that the three protocols are able to deliver data while having acceptable routing load regardless the malicious nodes percentage. In case of ARAN and ARANz, data delivery is almost guaranteed without affecting either the time required to obtain the routes or the number of hops in the selected paths. In AODV, however, APNH and ARAL slightly increase with increasing malicious node percentage since AODV can be exploited by malicious nodes so that non-optimal routes are chosen, while such exploitation in ARAN and ARANz is unfeasible.



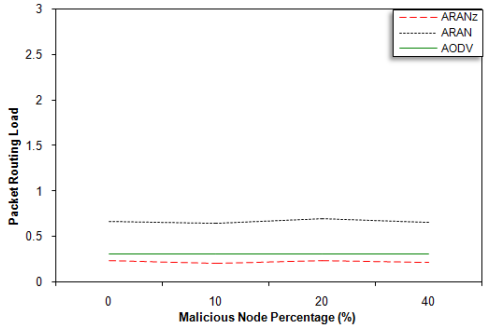

(a) Packet delivery fraction



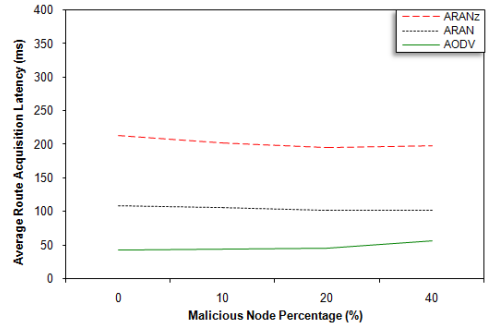

(b) Average path number of hops



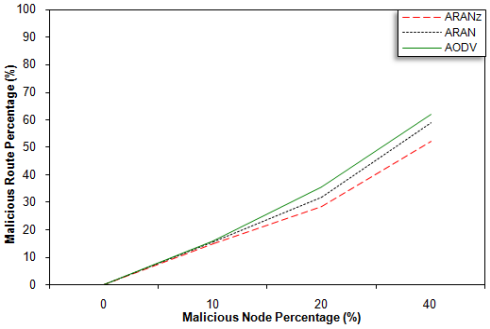

(c) Packet network load



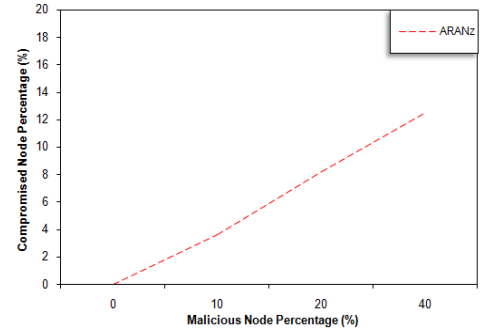

(d) Packet routing load



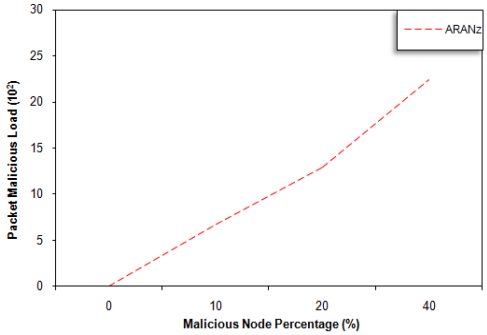

(e) Average route acquisition latency




(f) Malicious route percentage




(g) Compromised node percentage

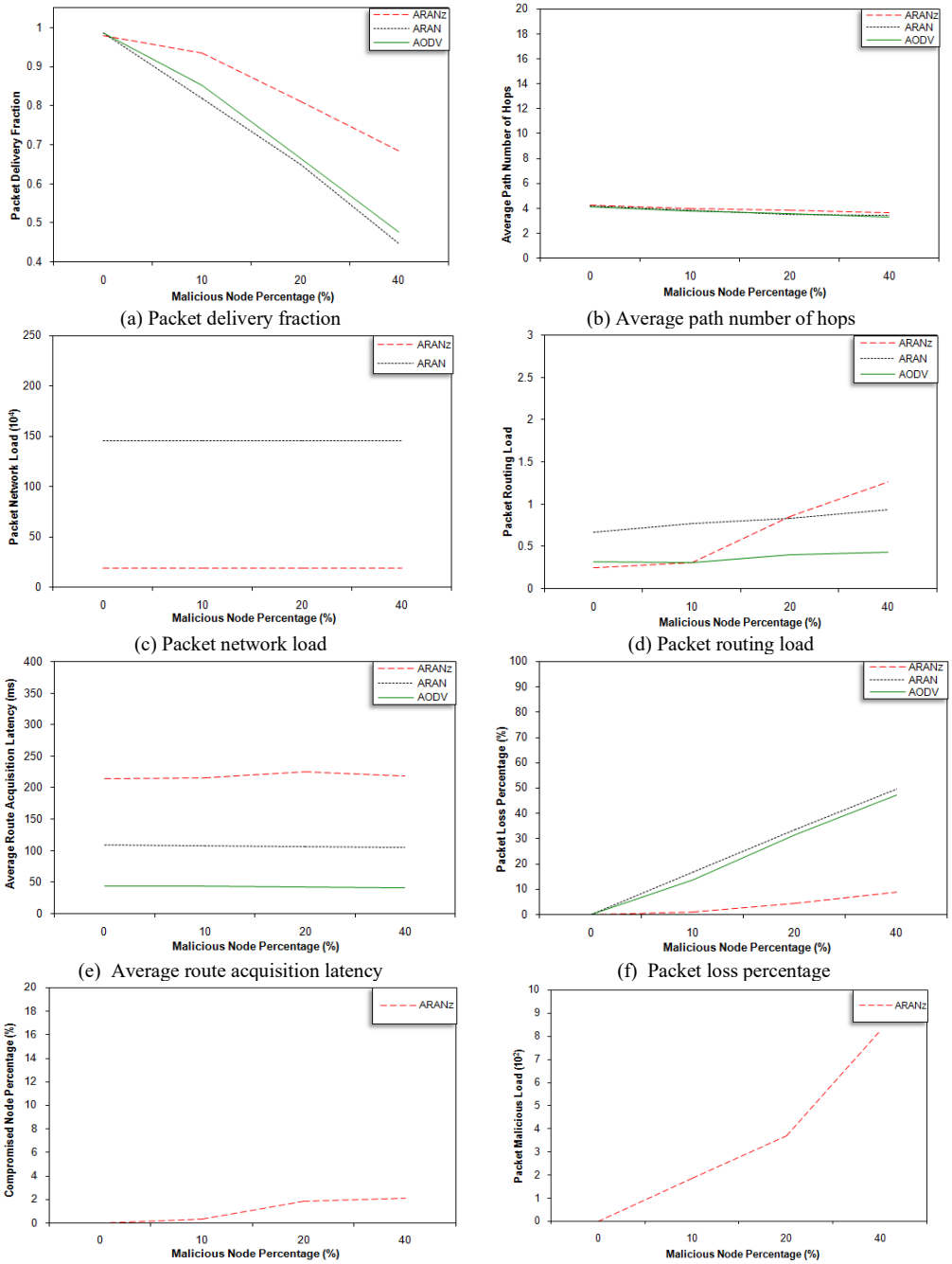



(h) Packet malicious load

Figure 2: Malicious node percentage effect considering modification attack

ARANz achieved the minimum PRL. In contrast to AODV and ARAN, ARANz does not send the RDP packets to the entire network, instead, these packets are forwarded using restricted directional flooding to the destination. 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 validate the preceding node digital signature and replace old signature with its own signature, besides the usual packet processing done by AODV. This signature verification and generation result 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.

Figure 2 (f) shows that MRP significantly increases for the three protocols upon increasing the malicious node percentage. Yet, the figure shows that upon using AODV, more fraction of routes has malicious nodes within them. When the malicious node sets the value of hop count field as 0, it convinces nodes to select the route that passes through itself; because AODV chooses the shortest paths. ARAN and ARANz, on the other hand, are not exploited in such way. The chosen route may pass through a malicious node but not forced to do so. Referring to Figure 2 (g and h), it is apparent that CNP and PML for ARANz increase as the misbehaving nodes increase. This implies that ARANz is efficient in discovering modification attacks and confirms our research hypotheses; i.e., utilizing the proposed misbehavior detection system improve ARANz performance and security.




(a) Packet delivery fraction
(b) Average path number of hops
(c) Packet network load
(d) Packet routing load
(e) Average route acquisition latency
(f) Packet loss percentage
(g) Compromised node percentage
(h) Packet malicious load

Figure 3: Malicious node percentage effect considering black hole attack

### 4.3. Malicious Node Percentage Effect Considering Black Hole Attack

The black hole attack is considered in this scenario. In this attack, malicious nodes dump all data packets that they receive.

From Figure 3 (b, c and e), it is obvious that the APNH, PNL and ARAL for the three protocols are generally not affected by the simulated percentage of malicious nodes. The almost constant APNH and ARAL indicate that the three protocols are able to discover the shortest paths without affecting the time required to obtain the routes even with increasing the malicious node percentage. PNL for ARAN and ARANz protocols has almost fixed values for the reason that packets initiated to update nodes certificates and maintaining network structure are sent regardless of the number of nodes dropping data packets.

It is noticeable from Figure 3 (a) that PDF decreases for the three protocols upon increasing the malicious node percentage. The decrease in PDF is justifiable as the malicious nodes in this scenario perform the black hole attack, they drop the data packets they receive. However, the figure assures that the decrease in PDF is slower and insignificant in ARANz, suggesting that ARANz is capable of isolating the black hole attackers and confirms our research hypotheses.

By looking at Figure 3 (d), we can observe that PRL for AODV and ARAN is approximately not affected by misbehaving node percentage. For ARANz, this metric slightly increases as the malicious nodes number increases since detecting malicious nodes in ARANz causes reinitiating RDP packets in a try to find another secure route, i.e. slightly increasing the routing overhead.

Figure 3 (f) shows that PLP increases for the studied protocols as the misbehaving node percentage increases. However, when simulating ARANz the increase in PLP is much slower. This assures that ARANz is efficient in detecting black hole attacks and justifies the increase in CNP and PML for ARANz with increasing the malicious node percentage (refer to Figure 3 (g and h)).

### 4.4. Malicious Node Percentage Effect Considering Grey Hole Attack

In this scenario, the grey hole attack is considered. In such attack, a misbehaving node arbitrarily drops data packets. To simulate this attack, when a misbehaving node receives a data packet, an arbitrary number between 0 and 1 is drawn. When the number is lower than 0.5, the node drops the data packet. Otherwise, the data packet is sent to the successor node.

As in the previous scenario, Figure 4 (b, c and e) shows that APNH, PNL and ARAL for the evaluated protocols are somehow not affected by the percentage of malicious nodes existing in the network. Figure 4 (a) shows that PDF decreases for the three protocols as the number of malicious nodes dropping data packets is increased. However, the decrease in PDF is slower in ARANz implying that ARANz is efficient in detecting grey hole attackers.

Figure 4 (d) shows that PRL for AODV and ARAN is not affected by malicious node percentage. On the other hand, this metric for ARANz slightly increases with increasing the malicious node percentage. This increase in PRL is due to reinitiating RDP packets as a result of detecting malicious nodes.

Looking at Figure 4 (f), it is clear that upon increasing the malicious node percentage PLP increases for the three protocols. However, upon using ARANz, the increase in PLP is much slower, which is an evidence that ARANz is efficient in identifying grey hole attackers and helps us answer our research question. This also justifies the increase in CNP and PML for ARANz with increasing malicious node percentage (refer to (Figure 4 (g and h)).

In comparison with the previous scenario (black hole attack effect), results of the conducted experiments show that the increase in PRL, CNP and PML for ARANz is slower in this scenario. This means that discovering grey hole attackers is more difficult and requires a longer time compared to discovering black hole attackers because grey hole attackers drop only some of the data packets they receive, so it takes longer time to detect them. Another point to mention here is that even though discovering grey hole attackers is slower than discovering black hole attackers, black hole attackers drop all packets they receive. Consequently, the increase in PLP and the decrease in PDF are almost the same in both cases.

### 4.5. Malicious Node Percentage Effect Considering Fabrication Attack

This scenario is performed to examine the result of conducting the fabrication attack. In this attack, misbehaving nodes periodically fabricate ERR packets with a specific probability. To simulate this attack, malicious nodes existing in the route between the source and destination nodes periodically draws a number between 0 and 1. When the drawn number is lower than 0.5, they send an ERR packets along the path toward the source to report false broken links.

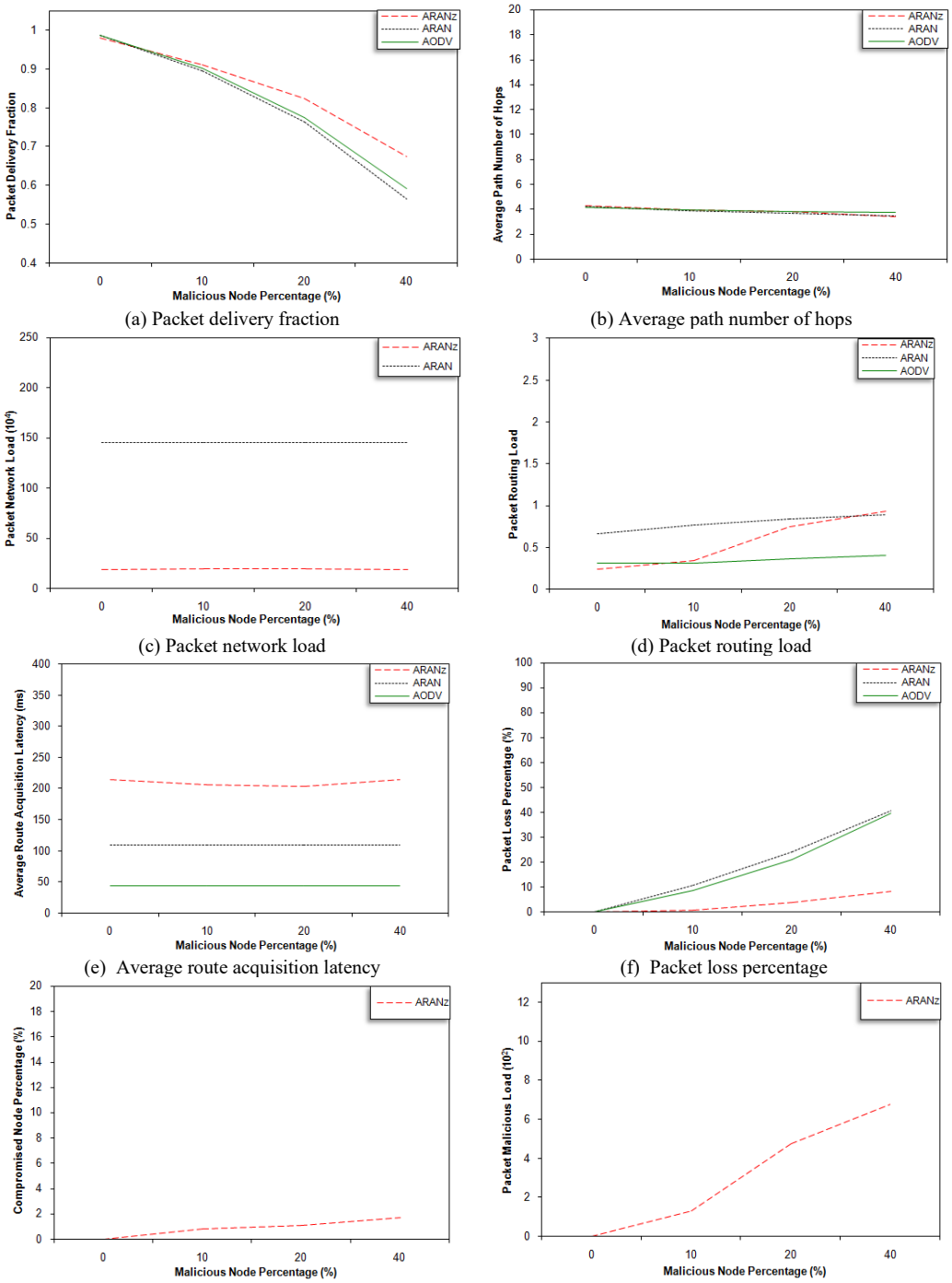
Figure 5(a) 5.93 shows that PDF decreases slightly for the three protocols as the malicious node percentage increases due to dropping some data packets as a result of receiving the fabricated ERR packets. However, the PDF for the three protocols is still above 90% even with the existence of large percentage of fabrication attackers.

As in the preceding three scenarios, Figure 5 (b and c) show that APNH and PNL for the evaluated protocols are, to some extent, not affected by attacking nodes percentage. This suggests that the three protocols are still able to discover the shortest paths even with the existence of some malicious nodes.

By looking at Figure 5 (d), it is noticeable that PRL for either protocol increases as the malicious node percentage increases. This increase in PRL is because of reinitiating RDP packets by the source node as a result of receiving the fabricated ERR packets.

Figure 5 (e) shows that ARAL for AODV and ARAN protocols is not affected by attacking nodes percentage. However, this metric for ARANz slightly increases with increasing the malicious node percentage. In ARANz, discovered malicious nodes are not included in future route selections which may result in choosing non-optimal paths that do not contain malicious nodes.

Figure 5 (f) shows that FEP increases for the three protocols upon increasing the malicious node percentage. But, the increase in FEP is much slower upon simulating ARANz, which indicates ARANz effectives in detecting and isolating nodes performing fabrication attack and answers our research question.




(a) Packet delivery fraction

(b) Average path number of hops

(c) Packet network load

(d) Packet routing load

(e) Average route acquisition latency

(f) Packet loss percentage

(g) Compromised node percentage

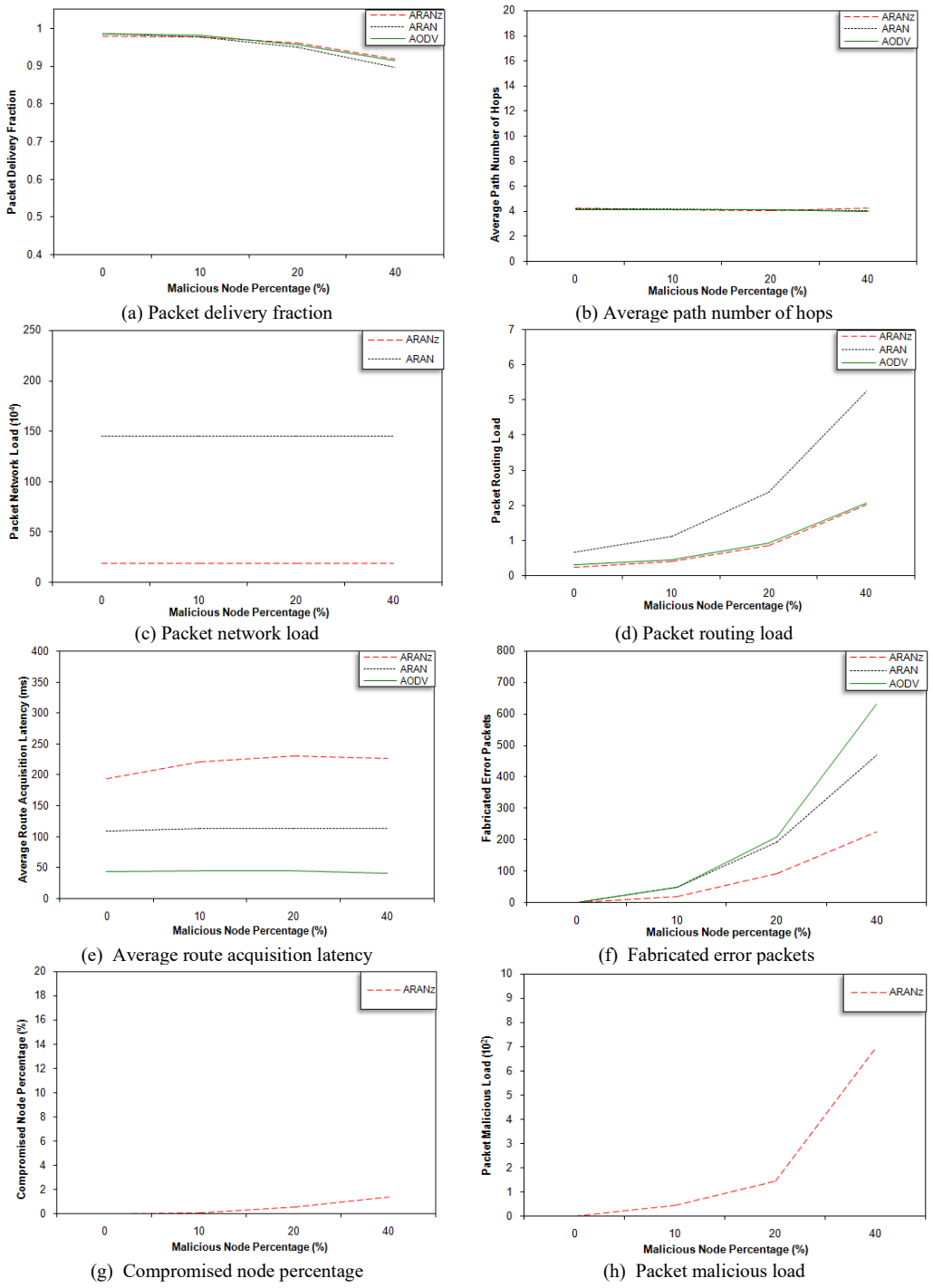
(h) Packet malicious load

Figure 4: Malicious node percentage effect considering grey hole attack

Figure 5 (g and h) show that CNP and PML increase as the malicious node percentage increases. In other words, as malicious node percentage increases ARANz demonstrates its effectiveness in distinguishing more and more malicious nodes.

### *4.6. Malicious Node Percentage Effect Considering Multi-Attack*

In this scenario, the effect of multi-attack is studied. In this attack, malicious nodes perform multiple attacks with a specific probability. To simulate multi-attack, malicious nodes perform modification, grey hole and fabrication attacks. The same details used to simulate each attack separately in the previous scenarios are used to simulate multi-attack. In other words, malicious nodes performing multi-attack illegally reset the hop count field to 0 in a received route discovery or route reply, if a drawn number is less than 0.5. They also drop a received data packet if a drawn number is less than 0.5 and periodically fabricate ERR packet if a drawn number is less than 0.5.



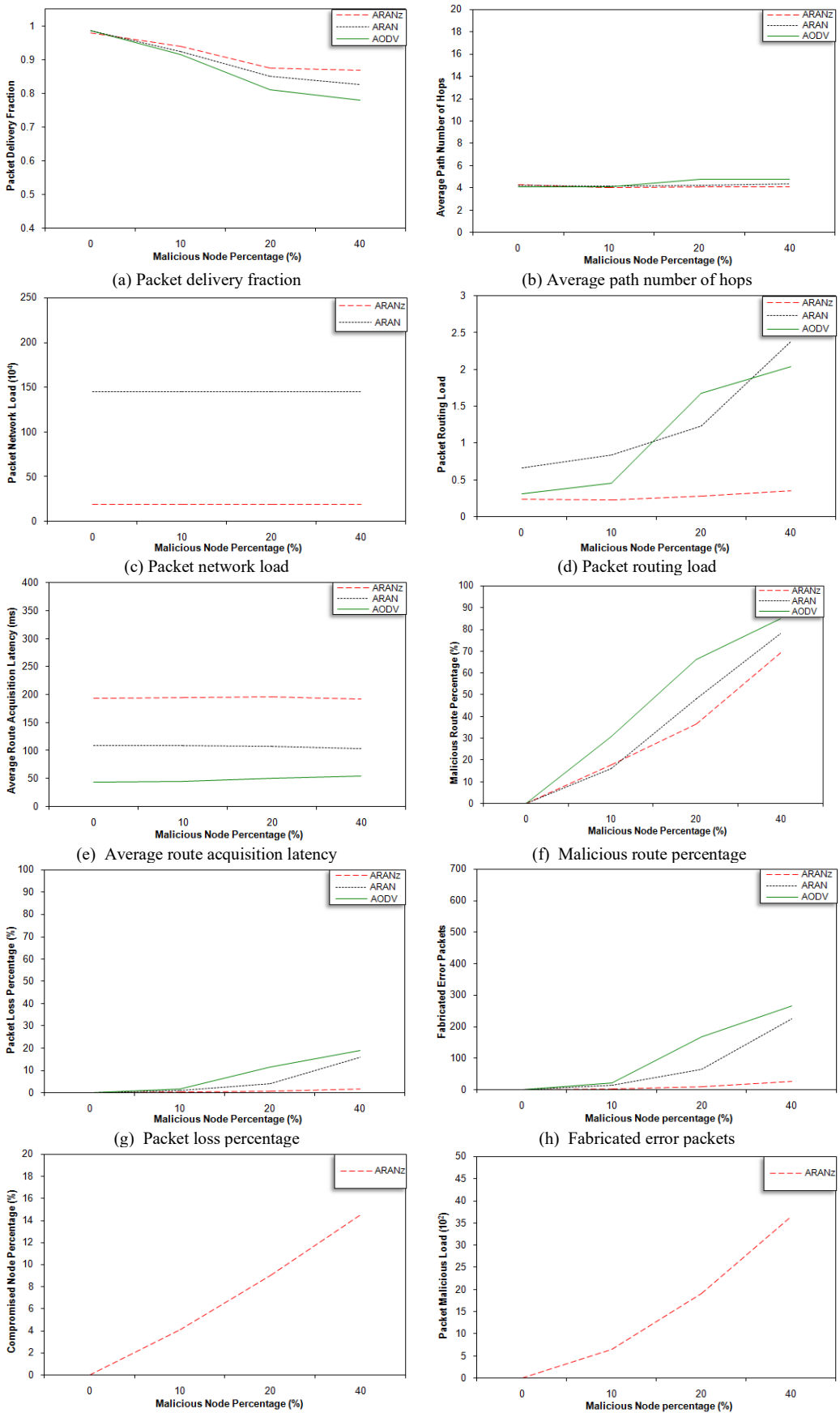

(a) Packet delivery fraction
(b) Average path number of hops
(c) Packet network load
(d) Packet routing load
(e) Average route acquisition latency
(f) Fabricated error packets
(g) Compromised node percentage
(h) Packet malicious load

Figure 5: Malicious node percentage effect considering fabrication attack

Referring to Figure 6 (a) it is clear that increasing malicious node percentage results in decreasing PDF for all protocols. This is mainly due to data packets dropped upon performing grey hole attack. The slower decrease in ARANz PDF is an indication that ARANz is effective in identifying and isolating multi-attack malicious nodes even if the simulated percentage is large.

Figure 6 (b) shows that APNH for AODV slightly increases upon increasing malicious node percentage. Misbehaving nodes can exploit AODV, via modification attack, so that non-optimal routes are chosen. ARAN and ARANz are not exploitable in this way.

It is conspicuous from Figure 6 (c) that malicious node percentage definitely does not affect PNL for ARAN and ARANz protocols. The reason behind the stable PNL is that updating nodes' certificates and positions is carried out regardless the number of existing malicious nodes.




(a) Packet delivery fraction

(b) Average path number of hops

(c) Packet network load

(d) Packet routing load

(e) Average route acquisition latency

(f) Malicious route percentage

(g) Packet loss percentage

(h) Fabricated error packets

(i) Compromised node percentage

(j) Packet malicious load

Figure 6: Malicious node percentage effect considering multi-attack

Figure 6 (d) reveals that PRL for all studied protocols increase upon increasing malicious node percentage. This increase in PRL is mainly due to reinitiating RDP packets by the source upon receiving the fabricated ERR packets. Also, it is apparent that ARANz attained the minimum PRL and ARANz has the slowest increase in PRL, which reflects ARANz effectiveness in detecting and isolating the fabrication attackers and assures our research hypothesis. Furthermore, it is clear that AODV is highly affected by the fabrication attack because the selected routes in AODV are forced to pass through malicious nodes via modification attack. After that, these malicious nodes start to fabricate ERR packets resulting in higher PRL. In ARAN and ARANz, however, routes are not forced to go through malicious nodes due to their robustness against the modification attacks.

Figure 6 (e) shows that ARAL for AODV slightly increases upon increasing malicious node percentage due to selecting non-shortest paths (since it is susceptible to modification attack). ARAL for ARAN and ARANz protocols is not affected by increasing attacking nodes percentage since they are robust against modification attacks.

Figure 6 (f) reveals that the MRP increases for the three protocols as the misbehaving nodes percentage increases. As the figure also shows, more routes with malicious nodes within them are used upon simulating AODV. When the attacker sets the hop count field to 0, it forces AODV to select the route passes through itself since AODV selects the shortest path.

Figure 6 (g) assures that the PLP increases upon increasing malicious node percentage due to dropping data packets via the grey hole attack. However, upon using ARANz, the increase in PLP is significantly slower indicating that ARANz is efficient in distinguishing grey hole attackers.

The FEP for the evaluated protocols increases upon increasing the malicious node percentage (as shown in Figure 6 (h)). However, the increase in FEP is much slower upon using ARANz, which illustrates that ARANz is effective in identifying and extracting nodes performing fabrication attack. Also, the increase in FEP is faster in AODV protocol since it is forced to use routes containing malicious nodes (via modification attack). Afterward, these nodes start sending fabricated ERR packets, resulting in higher FEP.

Figure 6 (i and j) show that as malicious node percentage increases ARANz demonstrates its effectiveness in detecting more and more malicious nodes, i.e. CNP and PML significantly increase as the percent of malicious nodes performing multi-attack increases.

## 5. Results Summary and Discussion

From the obtained simulation results, presented in the previous section, we can conclude that increasing malicious node percentage results in decreasing PDF and/or increasing PRL, MRP, PLP and FEP for the three protocols. In most cases, however, the decrease or increase in these metrics is much slower upon using ARANz. This assures ARANz efficiency in discovering and isolating the malicious nodes compared to the other two protocols due to the utilized misbehavior detection scheme. Consequently, this proves our research hypotheses; utilizing the proposed misbehavior detection system has really improved ARANz performance and security.

Table 5: Summary of the evaluated routing protocols

| Protocol / Criterion | AODV | ARAN | ARANz |
|---|---|---|---|
| **Approach** | Topology-based (reactive) | Topology-based (reactive) | Position-based (restricted directional flooding) |
| **Basic security** | - | Timestamps and certificates | Timestamps and certificates |
| **Proposal** | Uses next hop information kept on each node in the least number-of-hop route. | • Provides route discovery, setup and maintenance authentication.<br>• Prevents most attacks via using cryptographic certificates.<br>• Routing packets are authenticated at each hop from source to destination and vice versa. | • Deals with area as zones and introduces several LCAs.<br>• Involves initiating a PDP if destination position is unknown.<br>• Prevents most attacks via using cryptographic certificates.<br>• Control packets are authenticated at each hop from source to destination and vice versa. |
| **Advantages** | • No single point of failure.<br>• High robustness against nodes failure. | Robustness against most security attacks. | • Robustness against most security attacks.<br>• No single point of compromise and failure.<br>• Reduced packet overhead.<br>• High availability, robustness and scalability. |
| **Disadvantages** | • Relies on blind broadcasts to discover routes; resulting in higher control overhead and lower scalability.<br>• May be exposed to security vulnerabilities. | • Single point of compromise and failure; low availability and robustness.<br>• Scalability problem with the number of nodes inherited from AODV<br>• Increased packet overhead and route discovery delay compared to original AODV due to the encryption/decryption procedures. | • Synchronization among LCAs.<br>• Extra hardware (GPS).<br>• Extra delay to obtain the destination position. |

Table 6: Summary of the simulated performance and security evaluation

| Metric \ Protocol | AODV | ARAN | ARANz |
|---|---|---|---|
| Packet Delivery Fraction (PDF) | High | High | High |
| Average Path Number of Hops (APNH) | Almost the same as other protocols | Almost the same as other protocols | Almost the same as other protocols |
| Packet Network Load (PNL) | - | High | Low |
| Packet Routing Load (PRL) | Medium | High | Low |
| Average Route Acquisition Latency (ARAL) | Low | Medium | High |
| Malicious Route Percentage (MRP) | High | Medium | Low |
| Packet Loss Percentage (PLP) | High | High | Low |
| Fabricated Error Packets (FEP) | High | High | Low |
| Compromised Node Percentage (CNP) | - | - | Increased as malicious nodes increase |
| Packet Malicious Load (PML) | - | - | Increased as malicious nodes increase |

Moreover, as malicious node percentage increases, ARANz effectiveness in distinguishing and isolating malicious nodes is increasingly demonstrated by achieving higher CNP. This assures that ARANz is efficient in identifying and isolating malicious nodes performing modification attack against control packets, black hole and grey hole attacks against data packets, ERR packets fabrication attack as well as multi-attack against control and data packets. Discovering malicious nodes and excluding them from future routes may result in reinitiating RDP packets and choosing non-optimal paths that do not contain malicious nodes within them, hence, causing higher PML, PRL and ARAL.

Furthermore, results suggest that ARANz has accomplished scalability by retaining the minimum packet routing load even upon increasing the percentage of malicious nodes conducting different attacks. ARANz reduced packet routing load is a normal result of using restricted directional flooding to send RDP packets.

The price of ARAN and ARANz improved security is the increased routing load and latency in the route discovery process due to the performed cryptographic computations. Moreover, lower packet routing load of ARANz comes in the fee of increased latency in the route discovery due to destination position obtaining time.

Differing form ARAN, ARANz distributes load and trust by dealing with the area as zones and introducing several LCAs in each zone. ARANz has achieved robustness and high level of security and solved the single point of failure and attack problems by dealing with the area as zones and distributing trust among multiple LCAs. Accordingly, ARANz has achieved both security and scalability. Scalability has been assured by maintaining the minimum packet routing load within relatively large networks. This is a normal result of utilizing restricted directional flooding instead of broadcasting route discovery packets as in AODV and ARAN. Utilizing the misbehavior detection system helped ARANz to assure high level of security by identifying and isolating malicious nodes conducting different types of attacks. Hence, ARANz can be a good choice for Ad-Hoc networks established among students on a campus or peers at a conference, where pre-deployment of some keys and certificates is possible.

Table 5 highlights the key characteristics of the discussed protocols along with their advantages and disadvantages. Whereas Table 6 summarizes the main points concluded from the simulated evaluation.

## 6. Conclusions

One of the important issues to be tackled in Ad-Hoc networks is efficient routing since all nodes in the network act as both hosts and routers. Moreover, the nature of Ad-Hoc networks makes them prone to different attacks. AODV is an unsecure routing protocol, hence, its processing overhead is low. However, AODV broadcasts route discovery packets resulting in increasing packet overhead. Therefore, AODV scalability is low. ARAN is also a reactive protocol that sends the route discovery packet to all nodes in the network. Moreover, ARAN cryptographic certificates are utilized to detect erratic behaviors. However, using these certificates results in higher route acquisition latency as well as higher packet and processing overheads. This increase is due to the encryption/decryption procedures together with route request broadcast. The centralized trust and load are considered other problems of ARAN.

ARANz, on the other hand, proposes a hierarchal algorithm to improve the protocol performance and scalability through dealing with the area as zones. Via using several LCAs, ARANz achieves

robustness, enhances security and mitigates the single point of failure and attack problems. It also exhibits improved scalability and performance through the use of position-based routing.

In this research, a detailed discussion of the novel misbehavior detection system that has been integrated with ARANz protocol has been provided. Moreover, in this work a detailed performance and security evaluation has been conducted among AODV, ARAN and ARANz protocols. Our simulations show that ARANz is able to have superior performance even with having large percentage of malicious nodes conducting modification, black hole, grey hole and fabrication attacks. ARANz scalability has been proven through achieving the minimum packet routing load in all conducted scenarios. The expense is higher latency due to the required time for packet processing and authentication in addition to inquiring the destination position.

Accordingly, the obtained results confirm our research hypotheses; the proposed novel misbehavior detection system has certainly improved ARANz performance and security.

Hence, ARANz is considered a good choice for managed-open environments in which Ad-Hoc networks are established among students on a campus, peers at a conference, or even employees in a factory. In such environments, pre-deployment of some keys and certificates is possible. Moreover, the proposed misbehavior detection system can be incorporated into other existing non-secure routing protocols to help them protect the network and achieve security.

## 7. Future Works

The research presented in this work serves as a starting point for future research. First of all, more investigation is required in order to expansively evaluate ARANz protocol performance and security. For example, ARANz performance can be studied under different mobility models and different traffic generation applications. ARANz may also tested considering the case when nodes are not evenly geographically distributed. Moreover, ARANz security may be compared with other recent secure routing protocols.

Second, increased refinement and improvement of a routing protocol is always probable. ARANz may be modified to deal with different number and positions of LCAs in each zone, as well as using different zone shapes. One of the interested ideas that we are thinking of is extending our protocol to be implemented in 3-Dimensional environments such as buildings or war environments containing for example both vehicles and aircrafts.

As with other position-based routing protocols, there is a possibility of finding other techniques for nodes to be aware of their positions without using GPS. Additionally, on the subject of misbehavior mitigation, the proposed misbehavior detection system may be improved to detect other types of attacks. More attention may be given to authentication, key distribution and decreasing processing time and processing overhead of encryption approach.

Additionally, one of the important research limitations facing researchers in Ad-Hoc networks field is the difficulty to implement and test the network in real environment especially when the number of nodes is large. So, we look forward to implement and test our protocol via real implementation. However, this will require a large number of nodes and broad geographical areas to test its scalability.

Finally, this paper worked on one of the important Ad-Hoc network issues; i.e., security issue. However, there are still many open research concerns and challenges facing Ad-Hoc networks which worth exploring. These issues include, but not limited to, multicasting, energy-efficiency and provision of Quality-of-Service (QoS).

## Conflict of Interest

The authors declare no conflict of interest.

## References


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

[2] 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, **23**(3), 598-610, 2005.

[3] C. Perkins, E. Royer, "Ad hoc on-demand distance vector routing," 1999 IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, USA, 90-100, 1999.

[4] M. Belgaum, Sh. Musa1, M. Su'ud, M. Alam, S. Soomro, Z. Alansari, "Secured approach towards reactive routing protocols using triple factor in mobile ad hoc networks," Annals of Emerging Technologies in Computing (AETiC), **3**(2), 2019.

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

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

[7] H. Chen, Y. Xiao, X. Hong, F. Hu, J. Xie, "A survey of anonymity in wireless communication systems," Security and Communication Networks, **2**(5), 427-444, 2009.

[8] S. Seys, B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," International Journal of Wireless and Mobile Computing, **3**(3), 145-155, 2009.

[9] B. Saoud, A. Moussaoui, "New routing protocol in ad hoc networks," in 2019 International Conference on Computer Networks and Inventive Communication Technologies ICCNCT, 443-452, 2019.

[10] A. Pirzada, C. McDonald, "Reliable routing in ad hoc networks using direct trust mechanisms," In Cheng M, Li D. Advances in Wireless Ad Hoc and Sensor Networks, 133-159, 2008.

[11] A. Dorri, S. Kamel, E. kheyrkhah, "Security challenges in mobile ad hoc networks: A survey," International Journal of Computer Science & Engineering Survey (IJCSES), **6**(1), 15-29, 2015.

[12] Sh. Thapara, S. Sharmab, "Attacks and security issues of mobile ad hoc networks," in 2019 International Conference on Sustainable Computing in Science, Technology & Management (SUSCOM), Jaipur, India, 1463-1470, 2019.

[13] Z. Khan, A. Sharma, "Security aspects of MANETs: A review," International Journal of Computer Science and Mobile Computing, **8**(7), 40-44, 2019.

[14] F. Abdel-Fattah, Kh. Farhan, F. Tarawneh, F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs," in 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 28-33, 2019.

[15] M. Soni, B. Joshi, "Security assessment of routing protocols in mobile ad hoc networks," in 2016 IEEE International Conference on ICT in Business Industry & Government (ICTIBIG), 2016.

[16] M. Soni, B. Joshi, "Security assessment of SAODV protocols in mobile ad hoc networks," Data Science and Big Data Analytics, **16**, 347-355, 2018.

[17] J. Arshad, M. Azad, "Performance evaluation of secure on-demand routing protocol for mobile ad hoc networks," in 2006 IEEE Sensor and Ad Hoc Communications and Networks Conference (SECON), 2006.

[18] N. Luong, T. Vo, D. Hoang, "FAPRP: a machine learning approach to flooding attacks prevention routing protocol in mobile ad hoc networks,"

Wireless Communications and Mobile Computing, 2019. https://doi.org/10.1155/2019/6869307

[19] M. Abu Zant, A. Yasin, "Avoiding and isolating flooding attack by enhancing AODV MANET protocol (AIF_AODV)," Security and Communication Networks, 2019. https://doi.org/10.1155/2019/8249108

[20] M. Belgaum, Sh. Musa, M. Su'ud, M. Alam, S. Soomro, Z. Alansari, "Secured approach towards reactive routing protocols using triple factor in mobile ad hoc networks," Annals of Emerging Technologies in Computing (AETiC), **3**(2), 32-40, 2019.

[21] W. Alnumay, U. Ghosh, P. Chatterjee, "A trust-based predictive model for mobile ad hoc network in Internet of Things," Sensors, 2019. https://doi.org/10.3390/s19061467

[22] M. Boulaiche, "Survey of secure routing protocols for wireless ad hoc networks," Wireless Personal Communications, 2020. https://doi.org/10.1007/s11277-020-07376-1

[23] T. Zahariadis, P. Trakadas, S. Maniatis, P. Karkazis, H. Leligou, S. Voliotis, "Efficient detection of routing attacks in wireless sensor networks," in 2009 International Conference on Systems, Signals and Image Processing (IWSSIP), June, Chalkida, Greece; 1-4, 2009.