Secure Location-Aided Routing Protocols with Wi-Fi Direct for Vehicular Ad-Hoc Networks

Maen S. Saleh[1], Liang Dong[2], Ahmad F. Aljaafreh[1] and Naeem Al-Oudat[1]

[1]Department of Communication and Computer Engineering, Tafila Technical University, Tafila 66110 Jordan
[2]Department of Electrical and Computer Engineering, Baylor University, Waco, TX 76798 USA

Abstract: Secure routing protocols are proposed for the vehicular ad hoc networks. The protocols integrate the security authentication process with the Location-Aided Routing (LAR) protocol to support Wi-Fi Direct communications between the vehicles. The methods are robust against various security threats.

The security authentication process adopts a modified Diffie-Hellman key agreement protocol. The Diffie-Hellman protocol is used with a short authentication string (SAS)-based key agreement over Wi-Fi Direct out-of-band communication channels. It protects the communication from any man-in-the-middle security threats. In particular, the security process is integrated into two LAR routing schemes, i.e., the request-zone LAR scheme and the distance-based LAR scheme. We conduct extensive simulations with different network parameters such as the vehicular node density, the number of the malicious nodes, and the speed of the nodes. Simulation results show that the proposed routing protocols provide superior performance in secure data delivery and average total packet delay. In addition, the secure distance-based LAR protocol outperforms the secure request-zone LAR protocol.

Keywords: Security, Wi-Fi Direct, Mobility, Routing, Threat, VANETs.

1. Introduction

Vehicular ad hoc network (VANET) is a class of mobile ad hoc network (MANET), where a group of vehicles with high mobility provides connectivity to each other [1]. The intercommunication of the vehicular nodes can be through a direct transmission from the source to the destination if the destination is in the sources transmission range. It can also go through the intermediate nodes if the destination is outside the source’s transmission range [2].

The intelligent transportation system (ITS) uses the VANET technology to provide safety services to customers such as slow-down notifications, collision warnings, emergency notifications, and road enforcement [3]. A reliable intercommunication should be established for the safety services, because a disconnection may lead to a catastrophe [4]. In VANETs, different parameters degrade the reliability of the intercommunication between vehicles such as high-dynamic topology, intersections, traffic lights, road patterns, and signal blocking objects [5]. To overcome such limitations, the topology independent routing protocols, in particular, the position based routing protocols such as Location-Aided Routing (LAR), Greedy Perimeter Stateless Routing (GPSR), and Greedy Perimeter Coordinator Routing (GPCR) [6], [7], [8], [9], should be adopted for VANETs. In the proposed routing protocols, the physical locations of the vehicular nodes are found with the GPS service [10]. The position-based routing protocols provide a stable and reliable route to the destination, where the positions of the nodes are accurate through GPS service. One of the common communication methods for the VANET is the dedicated short-range communication (DSRC) that is based on the IEEE802.11p standard. It provides a reliable communication link between two vehicles. However, the DSRC technology has limitations in the cost of the additional dedicated hardware, the low channel bandwidth (10 MHz), and the low data rate (6-27 Mbps) [11]. The Wi-Fi Direct technology based on the IEEE 802.11n standard is used to establish a device-to-device (D2D) connection without the coordination of the access point [12]. It has been proven with real-time experiments that the Wi-Fi is a successful means of communication between vehicles in a VANET even at very high speed (i.e., 120 mph) [13]. Compared with DSRC, Wi-Fi Direct provides a channel bandwidth of 20 MHz, up to 250 Mbps data rates, and no additional hardware cost. The proposed routing protocols work with Wi-Fi Direct communication links to provide the required QoS requirements of the real-time data flow in the VANET.

The VANET is subject to many security threats that include altering GPS information, position cheating, identifier altering, snooping and spoofing, and man-in-the-middle attack (MITMA) [14], [15]. Hacking is a serious problem in the VANET due to information broadcasting, infrastructure less model, and high-dynamic topology changes [16], [17].

Accordingly, various secure routing protocols are proposed for the VANET [18], [19]. The geographical secure path routing (GSPR) protocol adds authentication and privacy to the geographic path routing (GPR) protocol through sharing geographic hashes to detect malicious nodes [20]. To deal with false-position security threats, digital signature and plausibility checks are used in a vehicle-to-vehicle secure position-based routing protocol [21], [22]. Hash message authentication code (HMAC) is integrated with the optimized link state routing (OLSR) to generate the secure OLSR (SOLSR) routing protocol [23], [24]. The protocol detects the snooping security threats through the use of symmetric and public cryptographic key. Integrity security service is provided for the VANET through the secure ad hoc on-demand distance vector (SAODV) routing protocol [25]. The hop count process is applied by the use of a hash chain, while the digital signature is used for authentication. In [26], a secure incentive scheme for fair and reliable cooperative downloading and forwarding packets between vehicles in highway

VANETs (SIRC) was proposed. Besides, secure downloading and forwarding, a reputation system to encourage cooperation and punish malicious vehicles was proposed. Simulation results show the efficiency of SIRC in high secure download success rate and low average download delay. To enhance security, efficiency and conditional privacy preserving in a highly dynamic VANET, an efficient conditional privacy-preserving authentication (CPPA) scheme was proposed in [27]. The proposed scheme adopts bilinear pairing to construct the identity-based signature to ensure the integrity and reliability of the forwarded message, Security analysis show that the proposed scheme outperforms other CPPA schemes in reducing the associated security overhead, while providing the required security requirements for the data flows. In [28], an integration between OoS and security units was proposed to provide a secure and reliable multi-constrained QoS aware routing algorithm for VANETs. The OoS unit adopts the ant colony optimization (ACO) technique, while the security unit was based on extending the VANET-oriented evolving graph (VoEG) model to perform plausibility checks on the routing control messages exchanged among vehicles. Simulation results show the ability of the proposed model in guaranteeing both QoS and security requirements for the data flows in VANETs. In [29], a combination between group signature and identity based (ID-based) signature was proposed to provide a secure authentication scheme for VANETs. Simulation results show the ability of the proposed scheme in providing cost effective, highly privacy preserving of user, efficient message authentication and verification for VANETs.

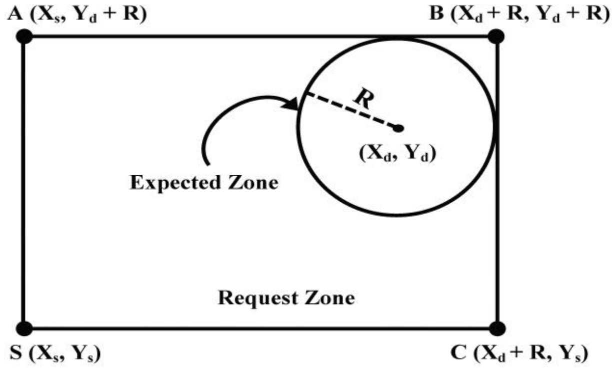


Figure 1. Request zone when Dist > R. Source node S is out of the expected zone of destination node D.

In this paper, we propose new routing protocols for the VANET that integrate the LAR with the security authentication process over Wi-Fi Direct data links between the vehicles. The routing protocols include the request-zone LAR (RLAR) scheme and the distance-based LAR (DLAR) scheme. The security unit adopts the Diffie-Hellman protocol with a short authentication string (SAS)-based key agreement over Wi-Fi Direct out-of-band communication channels. After conducting extensive simulations with different network parameters such as the vehicular node density, the number of the malicious nodes, and the speed of the nodes, simulation results show that the proposed secure LAR protocols outperform the existing non-secure LAR protocols in terms of secure data delivery and average total packet delay, and thus guaranteeing both security and QoS requirements for the real-time data flows. From the other side, secure distance-based LAR protocol outperforms the secure request-zone LAR protocol.

The key features of the proposed secure routing for the VANET are as follows:

1) The use of Wi-Fi Direct technology for data communication between vehicle nodes in high speed VANETs, thus providing the VANET with efficient node intercommunications (no access point coordination, no additional hardware, and high data rates).

2) The integration of the two LAR routing protocols with a security-authentication unit to provide a secure route in the VANET.

3) The integration of the Diffie-Hellman protocol with an SAS-based key agreement to provide a high level of security and make the VANET robust against threats such as the MITMA.

The rest of this paper is organized as follows. The RLAR protocol is proposed in Section 2. We describe the insecure Wi-Fi Direct RLAR and present the secure Wi-Fi Direct RLAR methods. The DLAR protocol is proposed in Section 3. We describe the insecure Wi-Fi Direct DLAR and present the secure Wi-Fi Direct DLAR methods. With extensive simulations, Section 4 gives the performance evaluation of the proposed routing protocols. Finally, conclusions are drawn in Section 5.

2. Request-Zone LAR (RLAR) Protocol

2.1 Expected zone and request zone

Suppose that each of the vehicular network nodes has its location information through the GPS service. The Expected Zone is a region in which the source (S) node expects the destination (D) node to be contained at some particular time [30]. Assume that node S knows that node D is at location L at time t0 and it travels at an average speed of v. From the viewpoint of S, the expected zone of node D at time t1 is the circular region of radius v(t1 - t0) centered at point L.

Node S knows its current location (Xs, Ys). It also knows the location of node D at time t0, i.e., (Xd, Yd), and the average speed v of D. Such information can be obtained by the auto-reply messages from the nodes. Node S wants to communicate with node D at time t1.

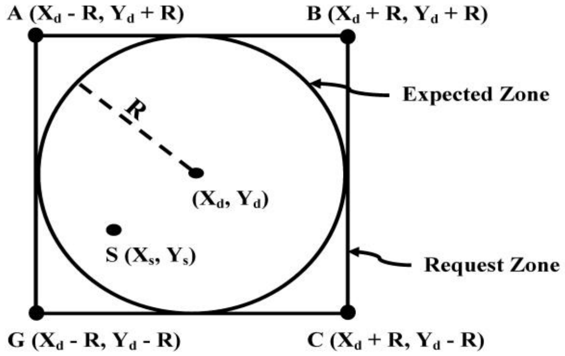


Figure 2. Request zone when Dist ≤ R. Source node S is in the expected zone of destination node D.

Accordingly, node S perceives the expected zone of node D at time t1 as a circular region with radius R = v(t1 - t0) and centered at location (Xd, Yd).

Node S evaluates the distance (Dist) between its location (Xs, Ys) and node D's location (Xd, Yd). With Dist, node S defines the Request Zone for the route request. It is the smallest rectangle that includes the current location of S and the expected zone of D such that the sides of the rectangle are parallel to the X and Y-axes. Given Dist and R, there are two situations:

1) If Dist > R, node S is out of the expected zone of node D. The request zone coordinates are shown in Fig. 1.

2) If Dist ≤ R, node S is in the expected zone of node D. The request zone coordinates are shown in Fig. 2.

2.2 RLAR with Wi-Fi direct communication

The LAR protocol depends on the nodes' location information to calculate the route from the source to the destination. We propose the request-zone LAR (RLAR) approach that uses the request zone information in routing.

In the RLAR protocol, Node S prepares the message for node D that includes:

1) Source coordinates (Xs; Ys),

2) The coordinates of the request zone (S, A, B, and C in Fig. 1) or (G, A, B, and C in Fig. 2),

3) Source and destination MAC addresses (e.g., vehicle plate numbers or engine serial numbers in a VANET),

4) The position of S corresponding to the request zone (e.g. inside or outside the request zone). Node S floods the message to its neighbors with the Wi-Fi Direct links. When a neighboring node B receives the message, it checks whether its location (Xb, Yb) is within the request zone. If node B is within the request zone, we have:

$$X_s \le X_b \le (X_d + R) \,\&\, Y_s \le Y_b \le (Y_d + R)$$

$$(X_d - R) \le X_b \le (X_d + R) \,\&\, (Y_d - R) \le Y_b \le (Y_d + R)$$

If node B is within the request zone, it checks whether the destination address is its address. If not, node B forwards the message to its neighbors. If node B is the destination, it generates an ACK message, i.e., a reply, and floods it. The reply message contains information about the current time and the destination node’s speed. Such information will be used by the source-node to define the request zone for future communication. If node B does not belong to the request zone, it discards the message. In addition, if a node receives the same message from a different node, it discards it. This protects the network from being congested.

Between any two vehicular nodes of the VANET, the Wi-Fi Direct technology is used as a communication means. Fig. 3 shows the communication protocol between a pair of nodes with Wi-Fi Direct. The first phase is the discovery process, where the two nodes perform channel-probing mechanism with the probe request and probe response control signals.

In the second phase, the group owner is negotiated through group-owner request, response, and confirmation. Once the group owner is specified, it acts as an access point for the connection. In the third phase, the Wi-Fi protected setup (WPS) is initiated by the group owner using the extensible authentication protocol signals such as EAPOL request and EAPOL response. Finally, the address configuration phase is initiated by the group owner by conducting the Dynamic Host Configuration Protocol (DHCP) [12].

2.3 Secure RLAR with Wi-Fi direct communications

According to the proposed protocol, we assume the following:

1) Any two trusted adjacent nodes belonging to the VANET can initiate an out-of-band channel. This channel is a trusted one such that it cannot be manipulated by the attackers;

2) For generating a shared security key, the trusted nodes that belong to the VANET use the Diffie-Hellman protocol with the common integer parameters such as the prime modulus (m) and the base (b);

3) Each node Ni has its own private key (ri), which is an integer not be exchanged. This key will be used to generate the public key in the network;

4) Each node Ni has its unique identification (ID) that can be considered as the MAC address in the network (e.g., the vehicle plate number);

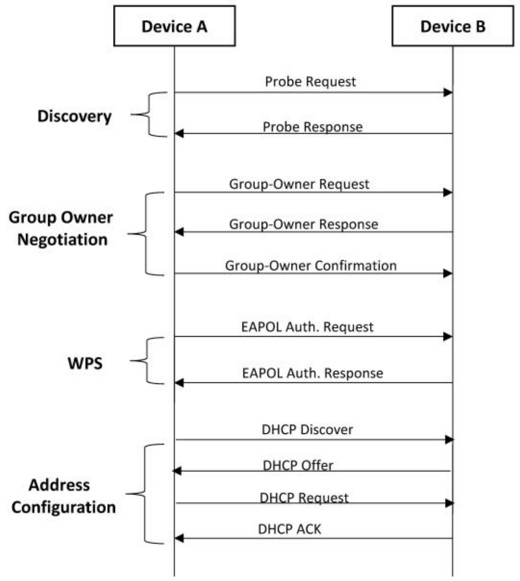


Figure 3. Communication protocol with Wi-Fi Direct.

5) Each node Ni can generate a k-bit random string (Ai). These k bits will be used to generate the authentication string (Si) of the short authentication string (SAS)-based key agreement protocol.

The Diffie-Hellman key agreement allows two vehicular nodes with no prior knowledge of each other to jointly establish a shared secret key [12]. The short authentication string (SAS)-based key agreement protocol involves minimal mutual authentication. It utilizes a cryptography commitment scheme. An efficient construction of a commitment is achieved by using a cryptographic hash function. Both nodes compute a hash value of the obtained shared key and compare the hash values via the secure out-of-band channel. The source node S performs the Diffie-Hellman key agreement protocol to generate its public key gs as in (1)

$$g_s = b^{r_s} \bmod(m) \qquad (1)$$

The source node S then generates a message m_s in the form of the concatenation of its public key g_s and the randomly generated k-bit string A_s as in (2)

$$m_s = g_s \,\|\, A_s \qquad (2)$$

In our proposed protocol, we use the commitment scheme of the cryptography schemes. On the one hand, a node is committed to a value and keeps it hidden from others (commit phase). On the other hand, it has the ability to unlock and reveal such a value later (open phase). An efficient construction of the commitment scheme can be achieved by using a cryptographic hash function [31].

The source node S uses its private key r_s with a cryptographic hash function H to compute the commitment c_s on the concatenation ms as

$$c_s = H(m_s, r_s) \qquad (3)$$

The source node S then includes the following information in the message that is sent to the destination:

1) The commitment c_s,

2) The source coordinates (X_s, Y_s),

3) The request zone coordinates (S A B C in Fig. 1) or (G A B C in Fig. 2),

4) Source and destination MAC addresses (ID_s, ID_d).

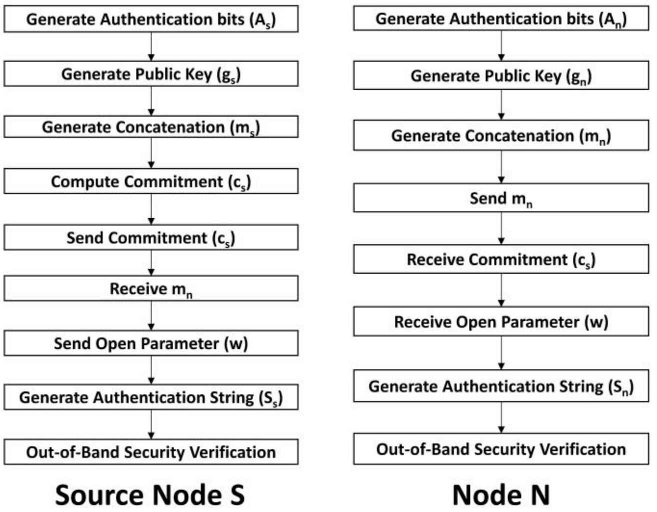

Generate Authentication bits (A_s)
Generate Public Key (g_s)
Generate Concatenation (m_s)
Compute Commitment (c_s)
Send Commitment (c_s)
Receive m_n
Send Open Parameter (w)
Generate Authentication String (S_s)
Out-of-Band Security Verification
Source Node S
Generate Authentication bits (A_n)
Generate Public Key (g_n)
Generate Concatenation (m_n)
Send m_n
Receive Commitment (c_s)
Receive Open Parameter (w)
Generate Authentication String (S_n)
Out-of-Band Security Verification
Node N

Figure 4. Security authentication model at source node S and node N.

The source node S floods the message to its neighbors with Wi-Fi Direct.

When a node N receives the message, it checks whether its location (X_n, Y_n) is within the request zone. If the node N is not within the request zone, it discards the message.

Otherwise, it generates its own concatenation m_n using formulas that are similar to (1) and (2). Node N then sends mn to the source node S (with the destination address ID_s). Once the source node S receives this message, it sends the open parameter w to node N (with destination address ID_n).

Before generating the shared security key, node S generates the k-bit authentication string S_s as

$$S_s = A_s \oplus A_n \tag{4}$$

where An is extracted from mn. Node N uses the open parameter w to reveal the commitment cs and extracts the k-bit string A_s from m_s. Node N then generates the k-bit authentication string S_n as

$$S_n = A_s \oplus A_n \tag{5}$$

Over the secure out-of-band channel, nodes S and N verify whether the two authentication strings match (S_s ?= S_n). The overall security-authentication model at the two parties (source node S and node N) is shown in Fig. 4.

If the two authentication strings do not match, the two parties stop the process of generating the security keys, and node N discards the message due to an MITMA. Therefore, node N will not be in the secure route to the destination. The source node S will use another adjacent node for the secure route. If the two strings match, both nodes S and N generate the shared key as

$$Key(s) = (g_n)^{r_s} \bmod(m) \tag{6}$$

$$Key(n) = (g_s)^{r_n} \bmod(m) \tag{7}$$

where Key(s) and Key(n) are the shared security keys at node S and node N, respectively. These two values are equal, i.e., Key(s) = Key(n). Note that, nodes S and N do not share such keys. They generate them using the shared public keys g_s and g_n.

Node N checks whether the destination address is its address. If not, it forwards the message that includes the request area coordinates to its neighbors. The same security authentication procedure repeats. If yes, node N generates an ACK message (reply) and floods it. The reply message contains information about the current time and the destination's speed. Such information will be used by the source for defining a new request zone for future communication. If a node receives the same message from a different node, it discards it.

3. Distance-Based LAR (DLAR) Protocol

3.1 DLAR with Wi-Fi direct communications

According to the above RLAR protocol, the route calculation is restricted by the boundaries of the requested zone. This may cause successive route disconnection. To overcome this limitation, we propose the distance-based LAR (DLAR) [30]. As shown in Fig. 5, the only restriction of the route calculation is the node's transmission range.

Assume the source node S knows the following information:

1) Its current location (X_s, Y_s) via GPS;

2) The location (X_d, Y_d) of the destination node D at some time t0.

The route discovery is initiated by node S at time t1, where t1 ≥ t0. The source node S calculates its distance from the location (X_d, Y_d), which is denoted as DISTs. It includes in the message sent to node D:

1) DISTs,

2) The coordinates of node D (X_d, Y_d),

3) Source and destination MAC addresses, e.g., vehicle plate numbers. The source node S floods the message to its neighbors through Wi-Fi direct.

When a node N receives the message, it calculates its distance DISTn from the destination coordinates (X_d, Y_d) and compares DISTn with DISTs. If DISTn ≤ DISTs, node N belongs to the route to the destination. Node N checks whether itself is the destination node. If it is not, node N replaces DISTs with DISTn in the message and forwards the message to its neighbors. If node N is the destination node, it generates an ACK message (reply) and floods it. This operation repeats until the message is received by the destination node.

If a node receives the same message from a different node, it discards it. This protects the network from being congested.

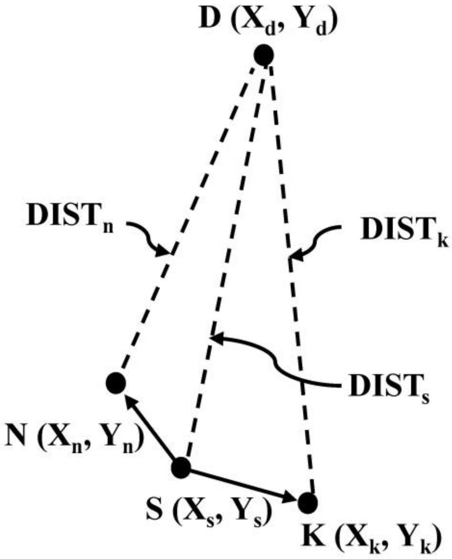


Figure 5. Distance-based LAR (DLAR) scheme.

3.2 Secure DLAR with Wi-Fi direct communications

We assume the following when integrating the security module in the DLAR:

1) The source node S knows its current location (X_s, Y_s) via GPS;

2) The source node S has knowledge about the location of node D (X_d, Y_d) at some time t_0. Route discovery is initiated by node S at time t_1 with ($t_1 \geq t_0$);
3) Each two trusted adjacent nodes in the VANET could establish an out-of-band channel. This channel is trusted and cannot be manipulated by the attackers;
4) The vehicular nodes use the Diffie-Hellman protocol to generate a shared security key with the common integer parameters such as the prime modulus (m) and the base (b);
5) Each node N_i has its own private key (r_i), which is an integer not to be exchanged. This key will be used to generate the public keys in the network;
6) Each node has its unique identification (ID) that can be considered as the MAC address in the network (e.g., the vehicle plate number);
7) Each node (Ni) can generate k-bit random string (Ai). This k-bit string will be used to generate the authentication string (Si) of the short authentication string (SAS)-based key agreement protocol.

Accordingly, the source node S performs the Diffie-Hellman key agreement protocol to generate its public key gs as in (1). The source node S then makes the concatenation ms of its public key gs and the randomly generated k-bit string A_s as in (2). The source node S uses its private key rs with a cryptographic hash function H to compute the commitment cs on the concatenation ms as in (3).

For the secure DLAR, the source node S calculates its distance from location (X_d, Y_d) which is denoted by DISTs. It includes the following information in the message that is sent to the destination:
1) The commitment cs,
2) DISTs,
3) The coordinates of the destination node D (X_d, Y_d),
4) Source and destination MAC addresses (ID_s, ID_d). The source node floods the message to its neighbors using Wi-Fi Direct.

When a node N receives the message, it calculates its distance ($DIST_n$) from the destination (X_d, Y_d). Node N determines whether it should be in the route by comparing $DIST_n$ with $DIST_s$. If $DIST_n > DIST_s$, it reasons that it is not in the route and discards the received message. If $DIST_n \leq DIST_s$, it knows, it belongs to the route and generates its concatenation m_n.

Node N sends m_n to the source node S with the destination address ID_s. Once the source S receives such message, it sends the open parameter w to node N with the destination address ID_n.

Before generating the shared security key, node S and node N generate the authentication string using (4) and (5), respectively. Note that, node N uses the open parameter w to reveal the commitment c_s and extracts the k-bit string A_s from m_s.

Over the secure out-of-band channel, node S and node N verify whether the two authentication strings match (S_s ?= S_n). If the strings do not match, the two parties stop the process of generating the security keys. Node N discards the message due to an MITMA. Node N is not in the secure route to the destination, and node S will use another adjacent node for a secure route. If the two strings match, both node S and node N generate the shared keys Key(s) and Key(n) according to (6) and (7), respectively. These two values are equal. Note that, the nodes do not share such keys. They generate them using the shared public keys g_s and g_n.

Node N checks whether the destination address is its address. If not, it forwards the message to its neighbors. The message includes the destination's coordinates (X_d, Y_d) and the distance $DIST_n$ instead of $DIST_s$. The operation repeats until reaching the destination. If node N is the destination node, it generates an ACK message (reply) and floods it.

If a node receives the same message from a different node, it discards the message. Such process protects the network from being congested.

The overall process of discovering the MITMA is shown in Fig. 6.

4. Simulation Results

Because the VANET environment is heterogeneous and dynamic, conventional network simulators are not sufficient for analyzing the real-time performance of the proposed routing protocols with security aspects. Besides, conventional network simulators such as ns-3 do not include geographic routing in their standard codes. They work well for wireless networks and MANET, but not for the VANET under consideration. In this research, we build our simulation models based on the .Net platform with its inherited object-oriented capabilities to analyze the performance of the proposed routing protocols.

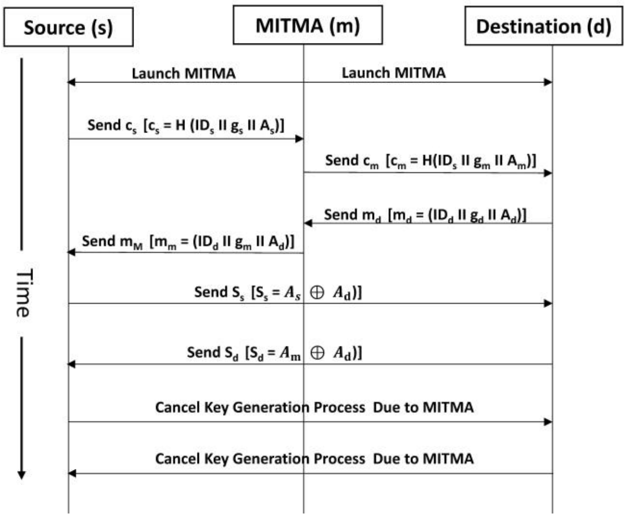

Source (s)
MITMA (m)
Destination (d)
Time
Launch MITMA
Launch MITMA
Send c_s [c_s = H (ID_s II g_s II A_s)]
Send c_m [c_m = H(ID_s II g_m II A_m)]
Send m_d [m_d = (ID_d II g_d II A_d)]
Send m_M [m_m = (ID_d II g_m II A_d)]
Send S_s [$S_s = A_s \oplus A_d$)]
Send S_d [$S_d = A_m \oplus A_d$)]
Cancel Key Generation Process Due to MITMA
Cancel Key Generation Process Due to MITMA

Figure 6. Discovery of the man-in-the-middle attack (MITMA) security threat.

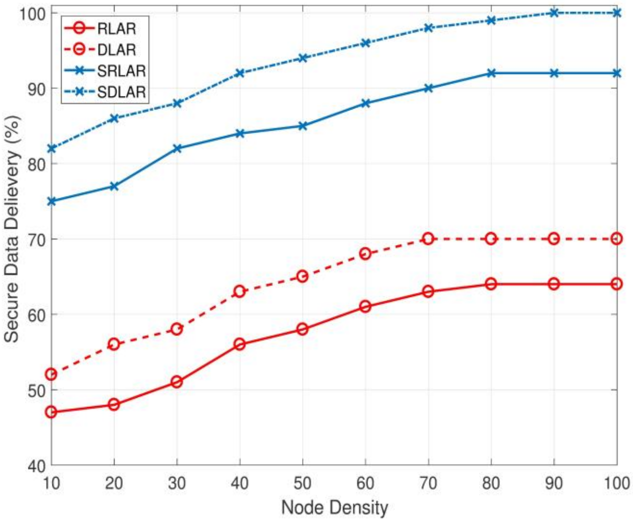


Figure 7. Effect of node density on secure data delivery for 10% malicious nodes and 5 units/sec node speed.

4.1 Motion model, system parameters and assumptions

In the simulations, we set the motion model, system parameters and assumptions as follows.

1) The number of vehicular nodes is set to be 10, 20, 30, …, N. In each simulation run, there are N/2 pairs of peer-to-peer communications, where the ith node is the source node and the (i + N/2)th node is the destination node, i = 1, 2, …, N/2.

2) The sending rate λ is 50 packets per second, with each node sending for 10 seconds (a total of 500 packets) to the destination. The inter-arrival time is exponentially distributed with a mean of 1/ λ.

3) The initial location of the nodes {(X, Y)} is randomly chosen. The nodes move continuously with velocity v that is uniformly distributed in [2, 40] units/sec. The nodes move in a square region of [1000 units x 1000 units].

4) The nodes change their direction after traveling a distance of d that is exponentially distributed with a mean of 25 units. When a node touches the region boundaries, it will "bounce back" and travel the remaining distance in the opposite direction.

5) Transmission range for each node is set to be 200 units.

6) For each simulation, the Diffie-Hellman security integer parameters, i.e., modulus m and base b, are randomly chosen and common to all the nodes. The private key r is randomly chosen for each individual node, and the k-bit string A is randomly generated by each node, where k = 10.

4.2 Node density effect

We study the performance of the proposed secure routing protocols regarding secure data delivery and average total packet delay on the node density. The number of nodes in the VANET region is chosen as N = 10, 20, 30, …, 100. The nodes' speed is set to be 5 units/sec. The percentage of malicious nodes that cause an MITMA is 10%.

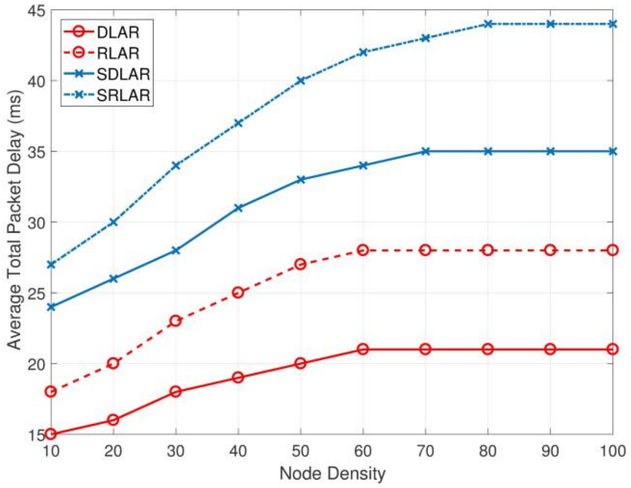
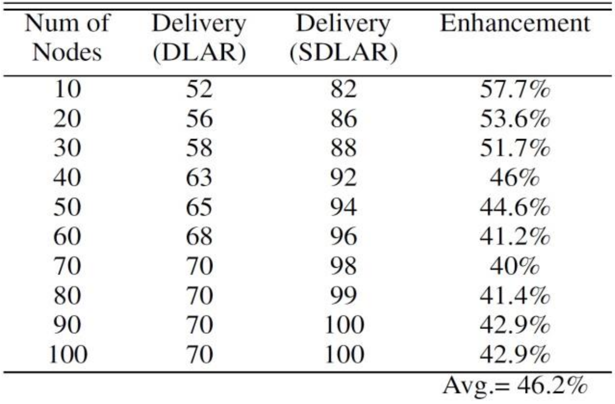


Figure 8. Effect of node density on average total packet delay for 10% malicious nodes and 5 units/sec node speed.

Fig. 7 shows the percentage of secure data delivery versus the number of nodes. Integrating the security module to the standard LAR protocol enhances the delivery of the data packets at the destination nodes. This is because the chances of dropping a packet due to the MITMA are reduced. Of the two secure routing protocols, the simulation results show that the secure DLAR protocol outperforms the secure RLAR protocol regarding secure data delivery. This is because the secure DLAR is only limited by the transmission ranges of the nodes whereas the secure RLAR is restricted by both the transmission ranges and the defined expected zones. Accordingly, the secure DLAR experiences fewer disconnections of the routes hence higher data delivery percentage.

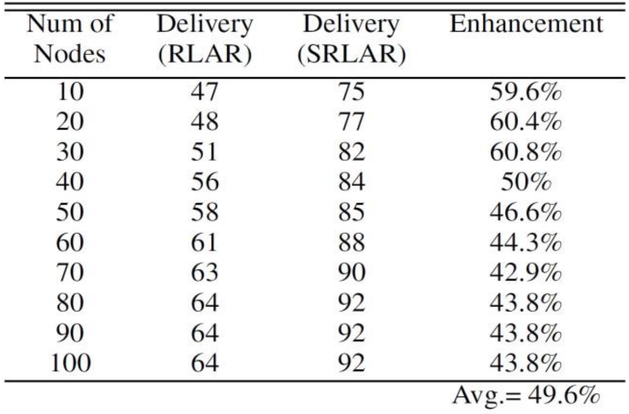
Fig. 8 shows the average total packet delay versus the number of nodes. The average total packet delay reflects the efficiency of finding a route from the source to the destination with the routing protocol. The simulation results show that the proposed secure routing protocols have a tradeoff of larger delays compared with the non-secure protocols. This is because the secure routing protocols have additional security association phases. Of the two proposed secure routing protocols, secure DLAR outperforms the secure RLAR regarding average total packet delay. Without the expected zone restriction, the secure DLAR experiences fewer route disconnections.

Table 1. Delivery (DLAR vs. SDLAR)



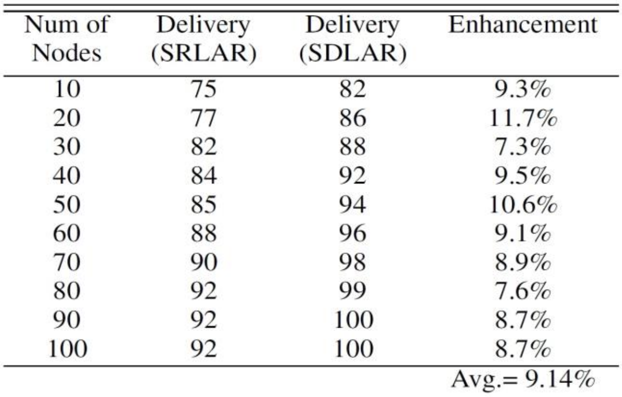
Num of Nodes	Delivery (DLAR)	Delivery (SDLAR)	Enhancement
10	52	82	57.7%
20	56	86	53.6%
30	58	88	51.7%
40	63	92	46%
50	65	94	44.6%
60	68	96	41.2%
70	70	98	40%
80	70	99	41.4%
90	70	100	42.9%
100	70	100	42.9%
			Avg.= 46.2%

Table 2. Delivery (RLAR vs. SRLAR)



Num of Nodes	Delivery (RLAR)	Delivery (SRLAR)	Enhancement
10	47	75	59.6%
20	48	77	60.4%
30	51	82	60.8%
40	56	84	50%
50	58	85	46.6%
60	61	88	44.3%
70	63	90	42.9%
80	64	92	43.8%
90	64	92	43.8%
100	64	92	43.8%
			Avg.= 49.6%

Table 3. Delivery (SRLAR vs. SDLAR)



Num of Nodes	Delivery (SRLAR)	Delivery (SDLAR)	Enhancement
10	75	82	9.3%
20	77	86	11.7%
30	82	88	7.3%
40	84	92	9.5%
50	85	94	10.6%
60	88	96	9.1%
70	90	98	8.9%
80	92	99	7.6%
90	92	100	8.7%
100	92	100	8.7%
			Avg.= 9.14%

Table 4. Delay (SRLAR vs. SDLAR)

To clarify the results, the data are analyzed in the following tables. Table 1 and Table 2 show the enhancement of the data delivery when integrating the security module in the LAR protocol. It is revealed that the secure DLAR improves the data delivery by an average of 46.2% over the non-secure DLAR and the secure RLAR improves by an average of 49.6% over the non-secure RLAR. Table 3 and Table 4 compare the secure DLAR with the secure RLAR. It is revealed that the secure DLAR enhances the data delivery by an average of 9.14% and reduces the average total packet delay by an average of 17.48% over the secure RLAR.

Num of Nodes	Delay (SRLAR) [ms]	Delay (SDLAR) [ms]	Enhancement
10	27	24	11.1%
20	30	26	13.3%
30	34	28	17.6%
40	37	31	16.2%
50	40	33	17.5%
60	42	34	19%
70	43	35	18.6%
80	44	35	20.5%
90	44	35	20.5%
100	44	35	20.5%
			Avg.= 17.48%

4.3 Security threat effect

We study the effect of the number of malicious nodes, particularly those cause the MITMA, on both data delivery and packet delay. The number of malicious nodes is set to be 2, 4, 6, …, 12. The number of vehicular nodes is fixed at 40, and the nodes' speed is 5 units/sec.

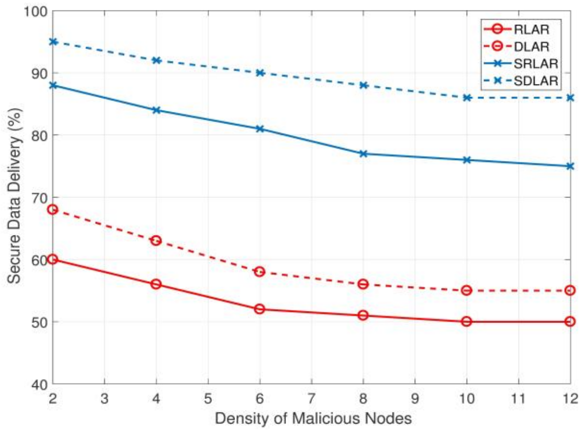


Figure 9. Effect of malicious nodes on secure data delivery for 40 vehicular nodes and 5 units/sec node speed.

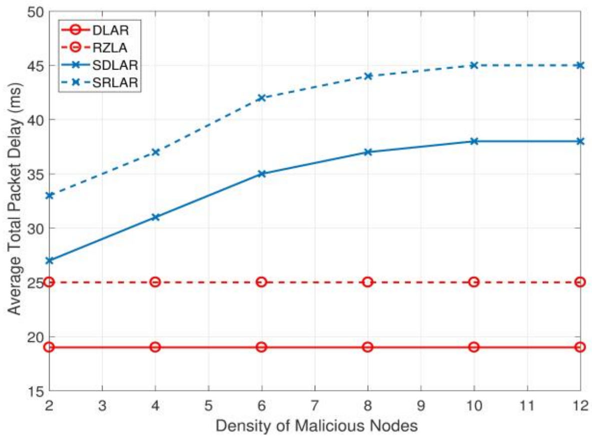


Figure 10. Effect of malicious nodes on average total packet delays for 40 vehicular nodes and 5 units/sec node speed.

Fig. 9 and Fig. 10 show that, with the secure routing protocol, a large number of malicious nodes has a negative effect on the VANET in reduced secure data delivery and increased average total packet delay. The secure DLAR outperforms the secure RLAR, which makes it more suitable for the VANET with security threats. Fig. 10 shows that the non-secure protocols have less packets delay and is irrelevant to the number of malicious nodes. This is because these protocols do not have any security association phase, which may lead to a catastrophe when facing security threats.

Table 5. Delivery (DLAR vs. SDLAR)

Num of Malicious Nodes	Delivery (DLAR)	Delivery (SDLAR)	Enhancement
2	68	95	39.7%
4	63	92	46%
6	58	90	55.2%
8	56	88	57.1%
10	55	86	56.4%
12	55	86	56.4%
			Avg.= 51.8%

Table 6. Delivery (RLAR vs. SRLAR)

Num of Malicious Nodes	Delivery (RLAR)	Delivery (SRLAR)	Enhancement
2	60	88	46.7%
4	56	84	50%
6	52	81	51.7%
8	51	77	55.8%
10	50	76	52%
12	50	75	50%
			Avg.= 51%

The data are analyzed in the following tables to clarify the simulation results on routing performances with different numbers of malicious nodes in the VANET. Table 5 and Table 6 show that the secure DLAR outperforms the non-secure DLAR in data delivery with an average 51.8% enhancement and the secure RLAR outperforms the non-secure RLAR with an average 51% enhancement.

Table 7. Delivery (SRLAR vs. SDLAR)

Num of Malicious Nodes	Delivery (SRLAR)	Delivery (SDLAR)	Enhancement
2	88	95	8%
4	84	92	9.5%
6	81	90	11.1%
8	77	88	14.3%
10	76	86	13.2%
12	75	86	14.7%
			Avg.= 11.8%

Table 8. Delay (SRLAR vs. SDLAR)

Num of Malicious Nodes	Delay (SRLAR) [ms]	Delay (SDLAR) [ms]	Enhancement
2	33	27	18.2%
4	37	31	16.2%
6	42	35	16.7%
8	44	37	15.9%
10	45	38	15.6%
12	45	38	15.6%
			Avg.= 16.3%

Table 7 and Table 8 compare the two secure LAR protocols regarding secure data delivery and average total packet delay, respectively. The tables show that, compared with the secure RLAR, the secure DLAR enhances the secure data delivery by an average 11.8% and reduces the packet delay by an average 16.3%.

4.4 Node speed effect

To show the effect of the node speed on the VANET performance metrics, i.e., secure data delivery and average packet delay, we simulate scenarios with the node speed v = 5, 10, 15, 20, …, 40 units/sec. The number of vehicular nodes in the VANET is 40, and the percentage of the malicious nodes is 10%, i.e., 4 malicious nodes.

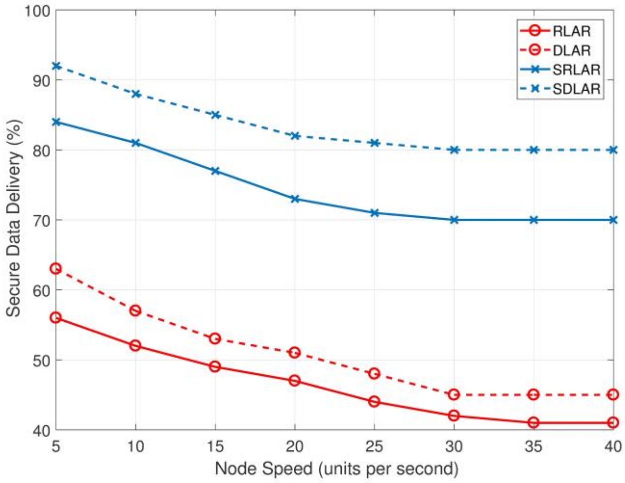


Figure 11. Effect of node speed on secure data delivery for 40 vehicular nodes and 10% malicious nodes.

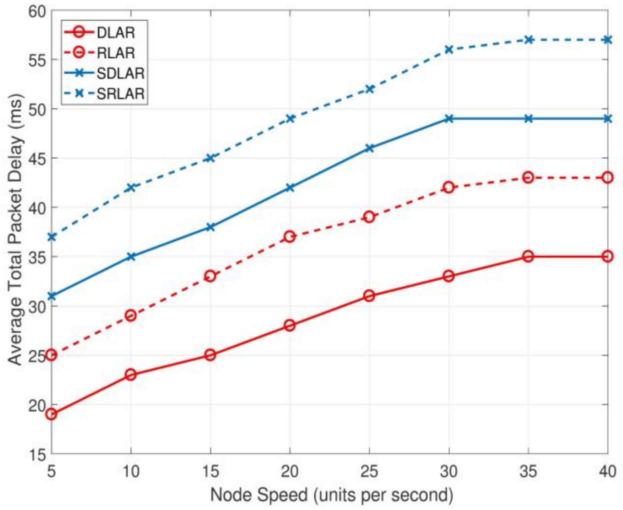
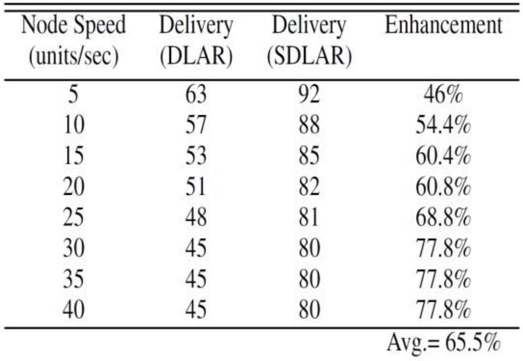


Figure 12. Effect of node speed on average total packet delay for 40 vehicular nodes and 10% malicious nodes.

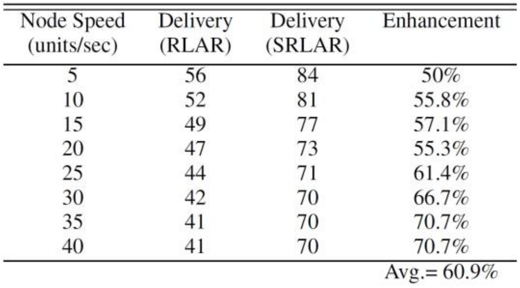
Fig. 11 and Fig. 12 show that the higher speed at which the nodes move, the less secure data delivery and the larger average total packet delay there are in the VANET. This is because the high mobility leads to the frequent route disconnection. Therefore, the overhead is high of finding a stable route from the source to the destination. The results show that the proposed secure LAR provides better data delivery with larger average total packet delay compared with the non-secure LAR. And, the secure DLAR outperforms the secure RLAR in data delivery and packet delay.

Table 9. Delivery (DLAR vs. SDLAR)



Node Speed (units/sec)	Delivery (DLAR)	Delivery (SDLAR)	Enhancement
5	63	92	46%
10	57	88	54.4%
15	53	85	60.4%
20	51	82	60.8%
25	48	81	68.8%
30	45	80	77.8%
35	45	80	77.8%
40	45	80	77.8%
			Avg.= 65.5%

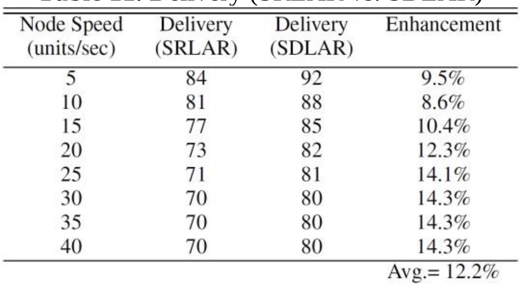
Table 10. Delivery (RLAR vs. SRLAR)



Node Speed (units/sec)	Delivery (RLAR)	Delivery (SRLAR)	Enhancement
5	56	84	50%
10	52	81	55.8%
15	49	77	57.1%
20	47	73	55.3%
25	44	71	61.4%
30	42	70	66.7%
35	41	70	70.7%
40	41	70	70.7%
			Avg.= 60.9%

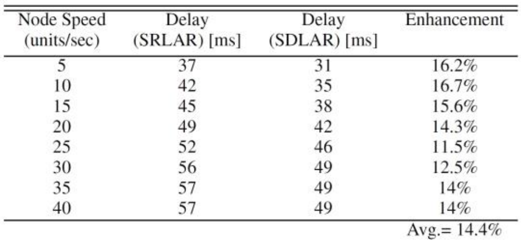
The performance of the VANET with different node speeds is clarified in the following tables. Table 9 and Table 10 show that the secure LAR routing protocols outperform the non-secure LAR routing protocols regarding secure data delivery with different node speeds. The records in the tables show that the secure DLAR outperforms the non-secure DLAR with an average 65.5% and the secure RLAR outperforms the non-secure RLAR with an average 60.9% in data delivery.

Table 11. Delivery (SRLAR vs. SDLAR)



Node Speed (units/sec)	Delivery (SRLAR)	Delivery (SDLAR)	Enhancement
5	84	92	9.5%
10	81	88	8.6%
15	77	85	10.4%
20	73	82	12.3%
25	71	81	14.1%
30	70	80	14.3%
35	70	80	14.3%
40	70	80	14.3%
			Avg.= 12.2%

Table 12. Delay (SRLAR vs. SDLAR)



Node Speed (units/sec)	Delay (SRLAR) [ms]	Delay (SDLAR) [ms]	Enhancement
5	37	31	16.2%
10	42	35	16.7%
15	45	38	15.6%
20	49	42	14.3%
25	52	46	11.5%
30	56	49	12.5%
35	57	49	14%
40	57	49	14%
			Avg.= 14.4%

Table 11 and Table 12 compare the secure DLAR and the secure RLAR regarding secure data delivery and average total packet delay, respectively. It is revealed that using the secure DLAR has an average 12.2% in enhanced data delivery and an average 14.4% in reduced packet delay.

The performance analysis for Fig. 11 and Fig. 12 shows that the secure LAR routing protocols outperform the non-secure LAR routing protocols regarding secure data delivery with different node speeds. It shows that the secure DLAR outperforms the non-secure DLAR with an average 65.5% and the secure RLAR outperforms the non-secure RLAR with an average 60.9% in data delivery. It also shows that using the secure DLAR has an average 12.2% in enhanced data delivery and an average 14.4% in reduced packet delay.

5. Conclusions

Two secure location-aided routing (LAR) protocols are proposed for the VANET. One routing protocol is based on the request zone and the other on the distance to the destination node. The protocols use Diffie-Hellman key agreement protocol with short authentication strings to establish secure communication links between vehicular nodes through Wi-Fi Direct. The VANET is therefore protected against security threats such as the MITMA. Extensive simulations are performed through the .Net framework to accommodate the dynamic geographic routing features. With different network densities, security threats and node speeds, simulation results show that the proposed secure LAR methods improve secure data delivery with a tradeoff in average total packet delay. Of the two proposed secure LAR methods, the secure DLAR outperforms the secure RLAR regarding both data delivery and packet delay.

References

[1] J. Harri, F. Filali, and C. Bonnet. Mobility models for vehicular ad hoc networks: a survey and taxonomy. IEEE Communications Surveys Tutorials, 11(4):19–41, Fourth 2009

[2] Ram Shringar Raw, DK Lobiyal, Sanjoy Das, and Sushil Kumar. Analytical evaluation of directional-location aided routing protocol for VANETs. Wireless Personal Communications, 82(3):1877–1891, 2015.

[3] Y. C. Chu and N. F. Huang. An efficient traffic information forwarding solution for vehicle safety communications on highways. IEEE Transactions on Intelligent Transportation Systems, 13(2):631–643, June 2012.

[4] Z. Li and C. T. Chigan. On joint privacy and reputation assurance for vehicular ad hoc networks. IEEE Transactions on Mobile Computing, 13(10):2334–2344, October 2014.

[5] M. Hashem Eiza, T. Owens, Q. Ni, and Q. Shi. Situation-aware QoS routing algorithm for vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 64(12):5520–5535, December 2015.

[6] K. Pandey, S. K. Raina, and R. S. Rao. Hop count analysis of location aided multihop routing protocols for VANETs. In International Conference on Signal Processing, Computing and Control (ISPCC), pages 68–73, September 2015.

[7] H. Saleet, R. Langar, K. Naik, R. Boutaba, A. Nayak, and N. Goel. Intersection-based geographical routing protocol for VANETs: A proposal and analysis. IEEE Transactions on Vehicular Technology, 60(9):4560–4574, November 2011.

[8] D. Tian, Y. Wang, H. Xia, and F. Cai. Clustering multi-hop information dissemination method in vehicular ad hoc networks. IET Intelligent Transport Systems, 7(4):464–472, December 2013.

[9] C. Wu, S. Ohzahata, and T. Kato. Flexible, portable, and practicable solution for routing in VANETs: A fuzzy constraint q-learning approach. IEEE Transactions on Vehicular Technology, 62(9):4251–4263, November 2013.

[10] N. Alam and A. G. Dempster. Cooperative positioning for vehicular networks: Facts and future. IEEE Transactions on Intelligent Transportation Systems, 14(4):1708–1717, December 2013.

[11] N. I. Shuhaimi, Heriansyah, and T. Juhana. Comparative performance evaluation of DSRC andWi-Fi Direct in VANET. In International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), pages 298–303, November 2015.

[12] W. Shen, B. Yin, X. Cao, L. X. Cai, and Y. Cheng. Secure device-to-device communications over WiFi direct. IEEE Network, 30(5):4–9, Sept./Oct. 2016.

[13] A. Tufail, M. Fraser, A. Hammad, Kim Ki Hyung, and Seung-Wha Yoo. An empirical study to analyze the feasibility of WIFI for VANETs. In International Conference on Computer Supported Cooperative Work in Design, pages 553–558, April 2008.

[14] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi. Vehicular security through reputation and plausibility checks. IEEE Systems Journal, 8(2):384–394, June 2014.

[15] M. Saleh and L. Dong. Real-time scheduling with security enhancement for packet switched networks. IEEE Transactions on Network and Service Management, 10(3):271–285, September 2013.

[16] R. Mishra, A. Singh, and R. Kumar. VANET security: Issues, challenges and solutions. In International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pages 1050–1055, March 2016.

[17] F. Qu, Z. Wu, F. Y. Wang, and W. Cho. A security and privacy review of VANETs. IEEE Transactions on Intelligent Transportation Systems, 16(6):2985–2996, December 2015.

[18] J. A. Martinez, D. Vigueras, F. J. Ros, and P. M. Ruiz. Evaluation of the use of guard nodes for securing the routing in VANETs. Journal of Communications and Networks, 15(2):122–131, April 2013.

[19] J. Toutouh, J. Garcia-Nieto, and E. Alba. Intelligent OLSR routing protocol optimization for VANETs. IEEE Transactions on Vehicular Technology, 61(4):1884–1894, May 2012.

[20] V. Pathak, D. Yao, and L. Iftode. Securing location aware services over VANET using geographical secure path routing. In IEEE International Conference on Vehicular Electronics and Safety, pages 346–353, September 2008.

[21] C. Harsch, A. Festag, and P. Papadimitratos. Secure position-based routing for VANETs. In IEEE 66th Vehicular Technology Conference, pages 26–30, September 2007

[22] Salim EL KHEDIRI1, Rehan Ullah Khan , Waleed Albattah. An optimal clustering algorithm-based distance aware routing protocol for wireless sensor networks, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 11, No. 3, December 2019.

[23] S. Jiang, X. Zhu, and L. Wang. An efficient anonymous batch authentication scheme based on HMAC for VANETs. IEEE Transactions on Intelligent Transportation Systems, 17(8):2193–2204, August 2016.

[24] Ali M A Abuagoub. IoT Security Evolution: Challenges and Countermeasures Review, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 11, No. 3, December 2019.

[25] S. Lu, L. Li, K. Y. Lam, and L. Jia. SAODV: A MANET routing protocol that can withstand black hole attack. In International Conference on Computational Intelligence and Security, volume 2, pages 421–425, December 2009.

[26] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen. Sirc: A secure incentive scheme for reliable cooperative downloading in highway vanets. IEEE Transactions on Intelligent Transportation Systems, 18(6):1559–1574, June 2017.

[27] Y. Xie, L. Wu, Y. Zhang, and J. Shen. Efficient and secure authentication scheme with conditional privacy-preserving for vanets. Chinese Journal of Electronics, 25(5):950–956, 2016.

[28] M. Hashem Eiza, T. Owens, and Q. Ni. Secure and robust multiconstrained qos aware routing algorithm for vanets. IEEE Transactions on Dependable and Secure Computing, 13(1):32–45, Jan 2016.

[29] D. Tiwari, M. Bhushan, A. Yadav, and S. Jain. A novel secure authentication scheme for vanets. In 2016 Second International Conference on Computational Intelligence Communication Technology (CICT), pages 287–297, Feb 2016.

[30] Young-Bae Ko and Nitin H Vaidya. Location-aided routing (LAR) in mobile ad hoc networks. Wireless networks, 6(4):307–321, 2000.

[31] Rafael Pass. On deniability in the common reference string and random oracle model. In Annual International Cryptology Conference, pages 316–337. Springer, 2003.