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

Maen S. Saleh
Tafila Technical University, Tafila 66110, Jordan
Email: maen@ttu.edu.jo

Abstract—Secure data transmission is one of the biggest challenges for Vehicular Ad Hoc Networks (VANETs) due to its dynamic and infrastructure-less characteristics. Such security services become a demand to provide safe and secure conversation between automobiles. In this paper, two optimized secure routing protocol for VANETs were proposed: 1) Secure Tilted-Rectangular-Shaped Request Zone Location-Aided Routing protocol (STRS-RZLAR); 2) Secure Cone-Shaped Request Zone LAR (SCS-RZLAR). Each proposed secure protocol integrates a security unit with an optimized shape request zone. The security unit in both protocols is a multi-layer unit that adopts two security agreement protocols: 1) modified Diffie-Hellman key agreement protocol; 2) short authentication string (SAS)-based key agreement protocol. The overall communication scheme is performed using Wi-Fi Direct out-of-band channels. The proposed secure protocols provide a reliable and secure data transmission between automobiles in a VANET and thus making it robust against man-in-the-middle attack (MITMA). Extensive simulations using three main network parameters: vehicular node density, number of malicious nodes and vehicle speed show that the proposed secure routing protocols provide superior performance regarding data delivery and normalized routing load (NRL) with a trade-off in average end to end packet delay. From the other side, Simulation results show that SCS-RZLAR protocol outperforms the STRS-RZLAR protocol regarding NRL and average end to end packet delay, while STRS-RZLAR protocol outperforms the SCS-RZLAR protocol regarding data delivery.

Index Terms—Security, VANETs, NPM, Wi-Fi Direct, MITMA, Routing.

I. Introduction

Vehicular Ad-hoc Networks (VANETs) is an expansion of Mobile Ad-hoc Networks (MANETs) [1]. Such networks are the foundation of next-generation intelligent transportation systems (ITSs) [2]. VANETs have been used to create intelligent systems using inter-vehicle communication (i.e., vehicle to vehicle communication V2V) and vehicle to road-side-unit (RSU) communication in a virtual-segmented road path as shown in Fig. 1 [3], [4]. VANETs offer different types of services that are mainly fall into two main categories: safety and comfort services. Safety services lead into reducing the road accidents and thus saving lives through exchanging warning messages regarding collisions, accident avoidance, traffic alerts, and secure emergency notifications. From the other side, VANETs provide its customers with the required services that make the travel more comfort and convenient such as peer-to-peer communications for sharing information, weather forecast, Internet browsing, and geo-location services [5].

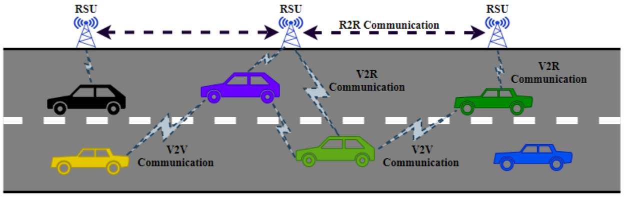

Fig. 1. ITS Communication Schemes using VANETs.

To provide a reliable and efficient connectivity between vehicular nodes in a VANET, different facts should be taken into considerations while designing the appropriate routing protocol such as the VANET dynamic topology, the unpredictable mobility patterns for the vehicular nodes, high mobility, frequent links disconnections, blocking objects, lane structure effect, traffic density due to peak time, driver's behavior, and security hacks opposing the VANET [6].

Due to the previous constraints, exact routing solutions (i.e. nonlinear definition of the path length [7], look-ahead feature [8], and k shortest paths [9]), approximated routing solutions (i.e. swarm intelligence [10]), MANET proactive routing protocols (i.e. FSR, DSDV, OLSR, CGSR, WRP, TBRPF, LSR, and TDR), MANETs reactive routing protocols (i.e. FSR, DSDV, OLSR, CGSR, WRP, TBRPF, LSR, and TDR), and MANETs hybrid routing protocols (i.e. ZRP and HARP) are not sufficient routing solutions for VANETs [11]-[13].

Accordingly, different routing solutions for VANETs were proposed. Based on the nature of the destination node, such protocols are classified into three different classes: multicast, broadcast, or unicast protocols [14]. According to the process of calculating the route to the destination, each routing class is classified into different subclasses of routing protocols including cluster-based protocols, position-based protocols, geo-cast-based protocols, and topology-based protocols [15], [16].

The position-based routing protocols outperform the other subclasses routing protocols in minimizing the overhead of finding the optimal route to the destination. In finding such optimal route, position-based protocols don't exchange any routing information with adjacent vehicular nodes. They don't even maintain any routing tables, but instead they perform the packets forwarding process

Manuscript received September 25, 2021; revised February 15, 2022.
doi:10.12720/jcm.17.3.156-166

according to the destination vehicle geographical position that is maintained by the position services received from satellites such as the global position system (GPS) and thus eliminating the overhead of rerouting process due to the high mobility and dynamicity in the VANET topology [17].

To provide an efficient communication scheme between vehicular nodes in a high dynamic VANET topology, different standards for communication scheme technologies were adopted by VANETs. One of the most common standards is the IEEE 802.11p. In the US, the federal communication commission (FCC) specifies the standards for the dedicated short-range communication (DSRC) such that it provides an efficient communication between vehicle nodes (vehicle to vehicle) in a VANET. The DSRC uses seven channels of 10 MHz bandwidth each that provide a range of data rates between 6 Mbps to 27 Mbps [18]. The limitations in the DSRC specifications (i.e., channel bandwidth, data rates, dedicated hardware) affects the overall communication mechanism between vehicle nodes and thus degrades the type of service provided by the VANET. From the other side, communication schemes based on WiGig and 5G technologies are inefficient when used in VANETs. Although WiGig provides a high data transmission rate (i.e., up to 7Gbps), its higher frequency range results in a short wavelength and thus short-range area coverage (i.e., maximum of 30 feet) [19]. From the other hand, 5G provides a flexible network management and high utilization for vehicle resources but the unsolved privacy issues in 5G technology makes it not fully deployed for VANETs and intelligent transportation systems (ITS) [20].

A new technology for peer-to-peer communication was defined by the Wi-Fi Direct alliance based on the IEEE 802.11n standard, where a pair of devices can directly be connected securely via the Wi-Fi Direct protocol without any access point (AP) coordination [21]. The main features of the Wi-Fi Direct (i.e., high channel bandwidth, high data rates, and low hardware cost) make it a reliable and efficient communication scheme between vehicular nodes in high speed VANETs [22].

The main characteristics of the VANET such as the transmission media (i.e., air), dynamic topology, high mobility of the vehicular nodes, frequent disconnections, data broadcasting, and infrastructure model increases the chances that the VANET becomes vulnerable to different subclasses of security attacks. Such attacks include DoS, DDoS, Jamming, Greedy behavior, Sybil, Wormhole, MITMA, Malware, and Blackhole attacks [23], [24]. The previous security threats affect the overall types of services provided by the VANET. They may lead into a catastrophe, where high percentage of accidents occurs when a driver is unable to identify the surrounding incidents [25]. Accordingly, security issues in VANETs (i.e., security hacks and security mechanisms) cached up the attention of researchers in recent years to the greater extent.

II. Related Work

To address the problem regarding security threats in VANETs, deep research studies being conducted. Anonymous Batch Authentication Scheme based on HMAC for VANET was proposed in [26]. The scheme provides an authenticated list of trusted nodes to be used in the route to destination. In [27], a framework based on trust to detect DDoS attacks in a VANET was proposed. The major trust elements in the evaluation of trust are frequency value statistics, trust hypothesis statistics, residual energy, trust policy, and data factor. The proposed algorithm enhances the security level of the VANET by avoiding the trespassers in the network. In [28], dedicated short-range communication (DSRC) & revocation methods were used for detecting DDoS attack in a VANET based on offender data transfer. According to the proposed infrastructure, the node that accepts security messages at a specific timestamp has been recognized as attacked. It can shield itself against DDoS and DoS attacks in the coming times.

In [29], a multi-phase detection algorithm based on bloom filter was proposed to detect spoofing security threat in a VANET. The detected malicious node by the filter will be announced to all nodes in the VANET by an alarm message, such that the nodes will not consider it in their secure routes. A trust management algorithm using the watchdog algorithm was proposed in [30] to detect malicious nodes in a VANET. The system recommends communicating the packets through high trust nodes which has been stored in a trust table. The trust level of the nodes in table will be updated according to the monitoring process of the node's behavior. In [31], authentication and privacy are added to the geographic path routing protocol (GPR) through sharing Geographic hashes. In [32], secure LAR (SLAR) and secure request-zone LAR (SRLAR) routing protocols are proposed for VANETs. The protocols integrate the security authentication process with the LAR protocol to support Wi-Fi Direct communications between the vehicles and protect the VANET from MITMAs.

In [33], a context-aware security mechanism based on a homogeneous continuous-time Markov chain (HCTMC) was proposed for VANETs. The approach defines a transition matrix based on different VANET characteristics that allows the VANET to adopt security defense strategies against different types of security hacks. Vehicular Security through Reputation and Plausibility Checks (VSRP) technique was proposed in [34]. The algorithm applies security services in a VANET through the exploitation of trust levels for nodes in the network based on reputation and plausibility checks.

In [35], a lightweight multi-factor authentication mechanism for integrity security service in VANETs was proposed. The mechanism used integration between unclonable functions and pseudo identities to provide an authenticated and robust communication scheme between vehicular nodes. In [36], an Enhanced Distributed Trust

Computing Protocol (EDTCP) for VANETs was proposed as a new distributed trust computing framework based on the investigation of the direct experience between neighboring vehicles in a VANET without using any recommendation system.

A Trust-Based Distributed Authentication (TDA) method that relies on a global trust server and vehicle behavior for avoiding collision attacks was proposed in [37]. This method grounds both inter-vehicular and intra-vehicular communication security in VANETs. A Secure Ant-based Multi-Constrained QoS routing algorithm (S-AMCQ) was proposed in [38]. The algorithm utilizes the Ant Colony Optimization (ACO) technique to calculate appropriate routes in VANETs depending on multiple QoS constraints dictated by the type of networking data transported by the VANET. In [39], a Trust Model integrated to the AODV protocol (TMAODV) was proposed to identify sinkhole nodes in a VANET and to avoid selecting them in the route selection phase.

In this paper, a multi-layer unit that adopts two security agreement protocols: 1) modified Diffie-Hellman key agreement protocol; 2) short authentication string (SAS)-based key agreement protocol was integrated into two optimized shape request zone LAR protocols: 1) tilted rectangular shaped request zone LAR protocol (TRS-RZLAR); 2) Cone-Shaped request zone LAR protocol (CS-RZLAR). The overall communication scheme is performed using Wi-Fi Direct out-of-band channels to provide a reliable and secure data transmission between automobiles in a VANET and thus making it robust against man-in-the-middle attack (MITMA).

The rest of the paper is organized as follows: The optimized LAR protocols (TRS-RZLAR and CS-RZLAR) are described in Section III. The Secure Optimized LAR Protocols using Wi-Fi Direct communication scheme are proposed in section IV. With extensive simulations, Section V gives the performance evaluation of the proposed secure routing protocols. Finally, conclusions are drawn in Section VI.

III. Optimized LAR Protocols

The conventional LAR protocol utilizes the location information that are provided by the GPS sensors to reduce the route search space into a small and predefined area zone named by request zone. Such limitation in the search space results in fewer route discovery requests [40] (i.e., vehicular nodes beyond the limits of the request zone discard the route-request messages). A pre-step in defining the request zone is to find a limited zone where the destination node is expected to be within at a specific time. Such zone is called the expected zone. By using the information provided by the GPS sensors (i.e., source node coordinates, destination node coordinates, and destination node average speed), the conventional LAR defines the expected and request zones and their coordinates for two cases (i.e., whether the source node belongs to the expected zone or not) as shown in Fig. 1 and Fig. 2 [32], [40].

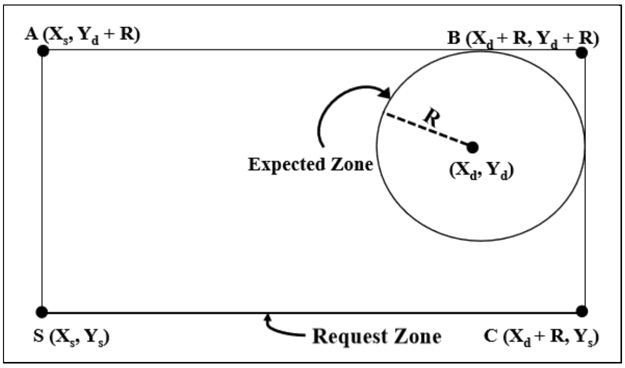

Fig. 2. Source S is outside the request zone.

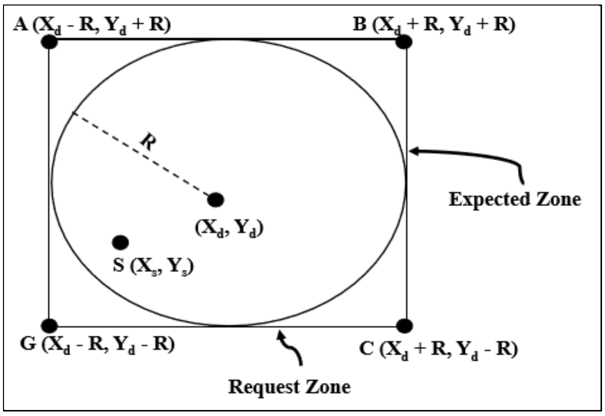

Fig. 3. Source S is inside the request zone.

However, two main limitations should be taken into consideration when using the LAR protocol. Firstly, the vehicular nodes in the VANET predict the destination position by assuming that the nodes don’t have a pure random mobility. The second limitation is that the route discovery process comes after the process of predicting the expected zone based on the destination information gathered by the GPS sensors. Due to high dynamicity and mobility of the vehicular nodes, such expectation may fail where the information about the destination node might be expired. Accordingly, an optimization of the expected and request zones should be taken into consideration such that the route discovery and delivery processes would be enhanced [41].

A. *Tilted-Rectangular-Shaped Request Zone LAR (TRS-RZLAR) Protocol*

The first optimized LAR protocol is the Tilted-Rectangular-Shaped Request Zone LAR protocol. Such protocol makes the request zone more flexible and independent than it in the conventional LAR. Instead of having a restriction that the coordinates of the request zone must be parallel with the real coordinates (X and Y), the request zone in the optimized Tilted one is dependent on the locations of both the source and destination vehicular nodes such that its sides are parallel to the shortest line connecting the two vehicular nodes (source and destination) as shown in Fig. 4 [42]. Such enhancement limits the route discovery process to a minimized request zone in comparison with the conventional LAR and thus the route disconnections due to the expiration of the destination node location are minimized (i.e., preserving the overall network performance metrics).

Upon defining the request zone coordinates, the source node performs the process of coordinate translation from the relative coordinates to the real ones (X and Y) as follows [42]:

$$x = x_s + \frac{x_1}{L} * (y_d - y_s) + \frac{y_1}{L} * (x_d - x_s) \quad (1)$$

$$y = y_s + \frac{x_1}{L} * (x_d - x_s) + \frac{y_1}{L} * (y_d - y_s) \quad (2)$$

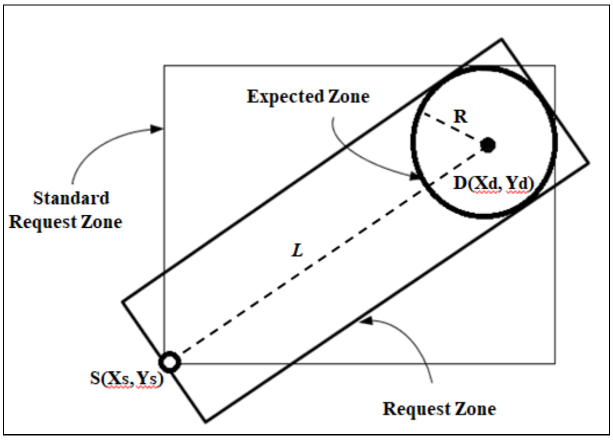

Fig. 4. TRS-RZLAR protocol.

B. *Cone-Shaped Request Zone LAR (CS-RZLAR) Protocol*

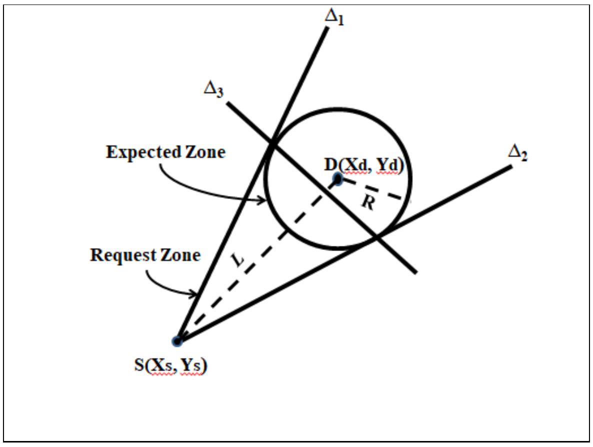

Fig. 5. CS-RZLAR protocol

According to the Cone-Shaped Request Zone LAR Protocol, the request zone is defined as a cone that has a root at the source node (S). In order to find whether a node Z (X_z, Y_z) belongs to the request zone or not, a plane with three main lines (Δ_1, Δ_2, Δ_3) as shown in Fig. 5. Accordingly, when the node Z receives a RREQ, it checks whether its coordinates belong to the predefined cone coordinates or not. The node Z is considered as part of the route (belongs to the request zone) if it satisfied one of two conditions:

1) If the node Z is within the expected zone that is:

$$\sqrt{(L - x_z)^2 + {y_z}^2} \leq R$$

2) If the node Z belongs to the triangle plane defined by the three lines (Δ_1, Δ_2, Δ_3) that is:

$$\boxed{\begin{gathered}((y_z - L - R) \leq 0\,)\&\& \\ ((y_z - x_z * \frac{L}{R}) \geq 0\,)\&\&\,((y_z + x_z * \frac{L}{R}) \geq 0)\end{gathered}}$$

Accordingly, if the node Z is not within the predefined request zone, it will discard the message. Otherwise, it broadcasts it unless it’s the final destination (D). One of the differences over the TRS-RZLAR is that the RREQ in this protocol will not transmit the coordinates of the predefined request zone, but instead it carries only the radius information.

IV. Secure Optimized LAR Protocols

In this paper, we adopt the secure communication scheme that we have proposed in [32] and we have applied it in [42] to the Cone-Shaped Request Zone LAR (CS-RZLAR) Protocol.

A. *Assumptions*

To implement a secure communication scheme between vehicular nodes using either the optimized TRS-RZLAR protocol or the CS-RZLAR protocol, the following assumptions have been taken into consideration [32], [42]:

1) The vehicular node in the VANET has the following attributes:
   - A unique ID to be considered as the MAC address of the vehicle node (i.e. plate number)
   - A non-shared unique integer private key (r).
2) Diffie-Hellman protocol parameters for VANET public-key generation process (i.e. prime modulus (m) and base (b)).
3) Each vehicular node generates a k-bit random string (A) that is used to generate the authentication string (S) of the short authentication string (SAS)-based key agreement protocol.
4) A reliable and efficient communication scheme between vehicular nodes using the out-of-band trusted channels provided by the Wi-Fi Direct technology.

B. *Communication Scheme*

The overall secure communication scheme passes through 4 phases: 1) public key generation; 2) commitment computation; 3) Route discovery; 4) Security association.

1) Public key generation phase

In order to generate the network’s public key, the multi-layer security unit at the source node (S) adopts in its first layer the Diffie-Hellman key agreement protocol. Such protocol allows any two independent unassociated vehicular nodes to negotiate on a secret-shared public key. Accordingly, the source node (S) uses its unique non-shared integer private key (rs) along with the predefined values of the Diffie-Hellman common integer parameters (ex. prime modulus (m) and the base (b)) to generate the source public key (g_s) as the following [32], [42]:

$$g_s = (b \wedge r_s) \bmod m \tag{3}$$

Once the public key (g_s) is generated, it will be passed to the second layer of the security unit.

2) Commitment computation phase

The second layer of the security unit adopts the short-authentication-string (SAS) based key agreement protocol that employs a minimum level of synchronization primitive for security aspects based on mutual authentication. In implementation, the mutual authentication process adopts a cryptographic commitment scheme through using an efficient cryptographic security service algorithm (i.e., hash functions) [43]. According to the commitment scheme, a vehicular node performs two main security operations: firstly, a commit operation, where the vehicular node is committed to a specific locked value (i.e., c). Secondly, a revel operation using a reveal parameter (i.e., w) will be performed by the vehicular node such that an unlock operation to the previously locked value (c) will be accomplished.

Upon receiving the public key (g_s), the SAS-based key agreement protocol at the source node applies a concatenation process to generate a message (m_s) as the following:

$$m_s = g_s || A_s \tag{4}$$

where A_s is the randomly generated k-bit string by the source node. The SAS-based key agreement protocol then uses the source private key (rs) with a cryptographic hash function H (i.e. SHA1) to compute the commitment (cs) parameter on the generated message by concatenation (ms) as the following:

$$c_s = H(m_s, r_s) \tag{5}$$

3) Route discovery phase

In this phase, the discovery of the nodes that are belonging to the request zone of the LAR protocol and might be part of the secure route to the destination is accomplished. In order to do that, The source node encapsulates the following information in a route request message: (1) Source location (X_s, Y_s); (2) The request zone coordinates: a) for the Standard LAR protocol (S A B C in Fig. 2) or (G A B C in Fig. 3); b) for TRS-RZLAR protocol (S L R in Fig. 4); c) for the CS-RZLAR protocol (S L R in Fig. 5); (3) The commitment (c_s); (4) Source and Destination ID numbers (ID_s, ID_d). The source node then broadcasts such request message to its neighbors using Wi-Fi Direct communication scheme.

According to Wi-Fi Direct, the communication scheme between any two nodes will pass four main phases as shown in Fig. 6: 1) Discovery phase, where channel probing mechanism is accomplished between the two interacted nodes using two probe control signals (request and response); 2) Group owner negotiations, where the owner of the group is negotiated between the communicated pair using three group-owner control signals (request, response, and confirmation). Upon specifying the group-owner vehicular node, it switches its chipset to an access point (AP) mode and starts working as an access point; 3) Authentication setup, where Wi-Fi protected setup (WPS) is initiated by the group owner using the extensible authentication protocol over LAN (EAPOL) signals; 4) Address configuration, where the group owner conducts the Dynamic Host Configuration Protocol (DHCP) to dynamically assign IP addresses to the communicated nodes [21], [32].

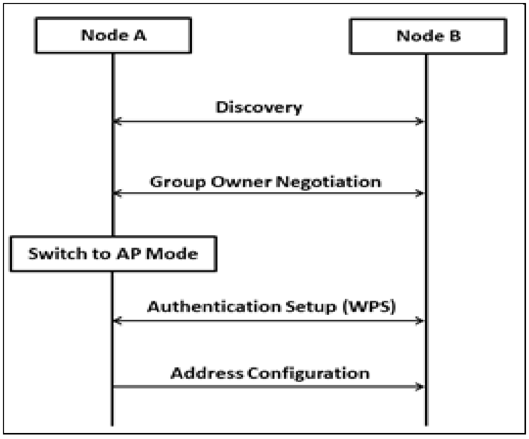

Fig. 6. Wi-Fi direct protocol

Upon receiving the RREQ message by an intermediate vehicular node (I), it checks whether its location (X_i, Y_i) is within the request zone or not. If it doesn't belong to the request zone, it discards the message (i.e. it will not be part of the route to the destination). Otherwise, it generates its own concatenation m_I using formulas that are similar to (1) and (2). Node I then send m_I to the source node S (with the destination address IDs). Once the source node S receives this message, it sends the open parameter w to node I (with destination address ID_I) and then the two parties begin the security association phase. The communication scheme is shown in Fig. 7.

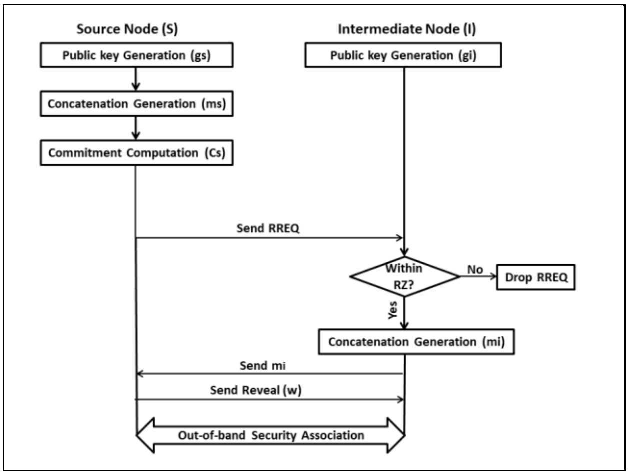
Source Node (S)
Intermediate Node (I)
Public key Generation (gs)
Public key Generation (gi)
Concatenation Generation (ms)
Commitment Computation (Cs)
Send RREQ
Within RZ?
No
Drop RREQ
Yes
Concatenation Generation (mi)
Send mi
Send Reveal (w)
Out-of-band Security Association

Fig. 7. Communication scheme

4) Security association phase

In this phase, the secure route to the destination will be discovered through detecting and excluding the malicious (MITMA) nodes from the route to the destination. The security verification process will be implemented over a secure out-of-band channel between a pair of intercommunicated vehicle nodes.

Upon receiving m_I , the source node extracts the randomly generated k-bit string by the intermediate node (A_I) and S generates the k-bit authentication string Ss as the following [32]:

$$S_s = A_s\, XOR\, A_I \qquad (6)$$

From the other hand, Node I uses the open parameter (w) to reveal the commitment cs and extracts the k-bit string (A_s) from (m_s). The node I then generates the k-bit authentication string $S_I$as the following [32]:

$$S_I = A_s\, XOR\, A_I \qquad (7)$$

The security verification process is performed by checking if both extracted string are identical or not. If they don't match (i.e., $S_s \neq S_I$), then node I will not be in the secure route to the destination due to the MITMA and then the source S will check another adjacent node. If the strings are identical (i.e., $S_s = S_I$), then then node I is a reliable node and will be in the secure route to the destination. Accordingly, the two nodes (S and I) will generate the security shared key (key$_{(s)}$ = key(I)) without exchanging it through the network as the following [32]:

$$key_{(s)=}\ {g_I}^{r_s}\ mod\ m\ \ (at\ node\ S) \qquad (8)$$

$$key_{(I)=}\ {g_s}^{r_I}\ mod\ m\ \ (at\ node\ I) \qquad (9)$$

The security association scheme is shown in Fig. 8. The process continues till an intermediate node finds that the destination address is its address. Accordingly, it acknowledges the source with an ACK messages containing information about its speed and current time for future communication.

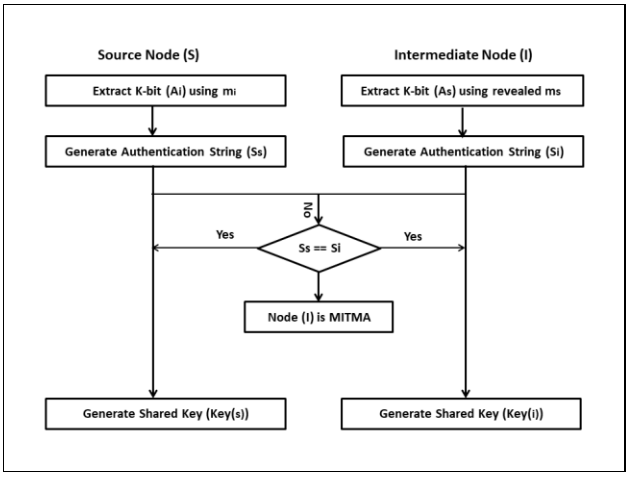
Source Node (S)
Intermediate Node (I)
Extract K-bit (Ai) using mi
Extract K-bit (As) using revealed ms
Generate Authentication String (Ss)
Generate Authentication String (Si)
No
Yes
Ss == Si
Yes
Node (I) is MITMA
Generate Shared Key (Key(s))
Generate Shared Key (Key(i))

Fig. 8. Security association scheme

V. SIMULATION & RESULTS

In this research, we build our simulation model using the QualNet simulator that is based on the GloMoSim used by Scalable Network Technologies (SNT) [44]. It's a planning, testing, and training tool that is used to design, optimize and analyze real-time heterogeneous networks. It's a discreet event, implemented in parallel simulation environment for complex systems (PARSEC) [45].

A. Motion Model and System Parameters

In our simulations, the motion model, system parameters and assumptions were set as the following:

1) The number of vehicular nodes (N) was set to be: [20, 40, 60, 80, 100].
2) A uniform distribution was used to obtain the initial locations of the nodes (X_0, Y_0).
3) The source node (S) and the destination node (D) are chosen randomly.
4) The nodes are moving in a square region [1000 m x 1000 m].
5) The nodes are moving continuously with an average velocity (v) between 4 m/s and 30 m/s.
6) A uniform distribution between [v- α, v+ α] was used to model the actual speed of the vehicles. We use α = 2 when v < 10 and α = 3 when v > 10.
7) Each node moves several movements. In each movement it travels distance (d) that is exponentially distributed with a mean of 20 m.
8) A random connection is established using constant bit rate (CBR) traffic.
9) The sending rate (λ) by the source is 40 packets/s and so, the inter-arrival time is exponentially distributed with a mean of (1/ λ).
10) The packet size is set to 64 bytes.
11) The channel rate is 2 Mbps according to IEEE 802.11.
12) The node transmission range is set to be 150 m.
13) The Diffie-Hellman parameters (modulus (m) and base (b) were randomly chosen.
14) The private key (r) is randomly chosen for each node.

B. Vehicular Nodes Density Effect

The effect of the node density on the network performance metrics (NPMs) was studied by varying the number of vehicular nodes (N) between 20 and 100 nodes with a step of 20 nodes in each simulation run (i.e. N={20, 40, 60, 80, 100}). The percentages of malicious nodes were set to be 5% of the total nodes in the VANET. The average velocity (v) is set to 12 m/s (i.e. α = 3 and a uniform distribution between [9, 15] was used to model the actual speed of the vehicles). The network performance metrics to be studied in this simulation are: 1) average data delivery; 2) routing overhead in terms of normalized routing load (NRL); 3) average end-to-end packet delay (ms).

Fig. 9 shows the enhancement achieved in data delivery by the secure LAR protocols over the insecure ones. Such result is due to the detection of the MITMAs and thus making the network robust against data packet dropping. The simulation results also show that the STRS-RZLAR protocol outperforms the SCS-RZLAR in data delivery. Such result is due to the limitations in the size of the request zone for the SCS-RZLAR that minimize the number of vehicle nodes in the zone. The effect of the size of the request zone on data delivery for the insecure LAR protocols is reflected by the simulation results, where Standard-LAR outperforms all other insecure protocols due to its request-zone size (i.e. the biggest size). The results also show that the data delivery for all protocols will be enhanced for higher values of node density, where the probability of finding a route to destination increases (i.e. less route disconnections).

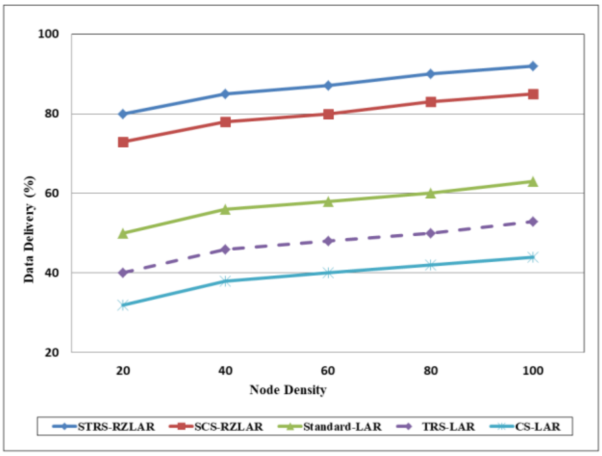

Fig. 9. Effect of node density on data delivery. 5% malicious nodes; 12 m/s node speed

The second NPM to be studied in these simulations is the normalized routing load (NRL). NRL is defined as the quantity of routing packets being transmitted per packet sent to the destination. It also assumes that each forwarded packet as one transmission. NRL is immensely associated with the number of the path or link changes or disconnection that happened during the simulations.

The NRL is calculated as follows:

$$NRL = \frac{NumberOfRoutingPacketsSent}{NumberOfDataPacketsRecieved} \qquad (9)$$

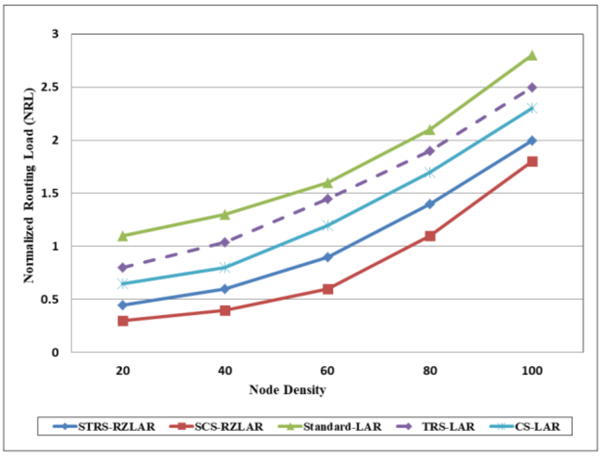

Fig. 10. Effect of node density on NRL. 5% malicious nodes; 12 m/s node speed.

Fig. 10 shows that the secure routing protocols outperforms the insecure ones in terms of NRL. Such enhancment is due to the exclusion of the MITMAs from the route to the destination and thus minimizing the number of route disconnections (i.e. less RREQ packets). Over the secure protocols, the results show the efficiency of using the SCS-RZLAR protocol in minimizing the routing overhead. Such enhancement is due to the improvement in the shape of the SCS-RZLAR request zone that has smaller size than the STRS-RZLAR request zone. Such improvement limits the number of RREQ broadcasts to the nodes in such smaller zone (i.e. less routing overhead). The results also show that the NRL for all protocols increases (more overhead) for higher values of node density, where the number of nodes in the request zone increases (i.e. more RREQ broadcasts).

The last NPM to be studied in these simulations is the average total packet delay. Simulation results show that the proposed secure routing protocols have a trade-off of larger delays compared with the non-secure protocols as shown in Fig. 11. Such result is due to the overhead of the security association phase adopted by the secure protocols. Of the two proposed secure routing protocols, results show that the SCS-RZLAR protocol outperforms the STRS-RZLAR regarding average total packet delay. Such enhancement is due to the improvement in the size of the SCS-RZLAR request zone that limits the number of RREQ broadcasts (i.e. less overhead delays).

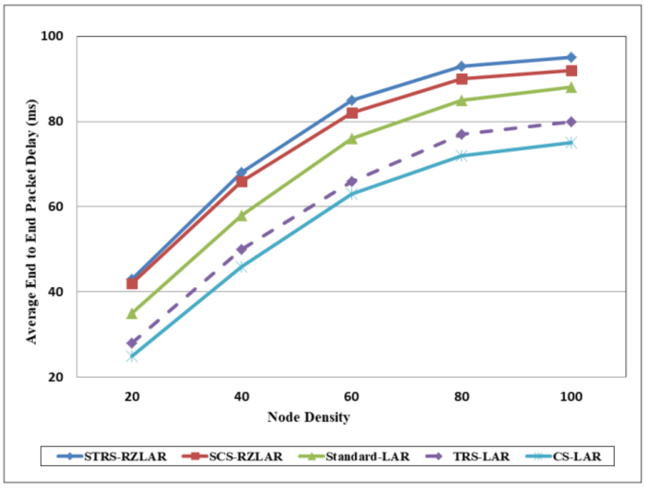

Fig. 11. Effect of node density on average end-to-end packet delay. 5% malicious nodes; 12 m/s node speed

C. *MITMA Effect*

In this section, we studied the effect of the MITMA on the network performance metrics (delivery, NRL, and end-to-end packet delay). Simulations were performed over a VANET of 60 vehicular nodes by varying the number of malicious nodes (Z) from 5% to 25% of the total number of vehicular nodes (N) with a step of 5% (i.e. Z= {3, 6, 9, 12, 15}). The average velocity (v) is set to 12 m/s (ex. α = 3 and a uniform distribution between [9], [15] was used to model the actual speed of the vehicles). Fig. 12 and Fig. 13 show the negative effect of large number of MITMA nodes on the data delivery and the normalized routing load NPMs. The results also show the enhancement achieved by the secure protocols on such metrics over the insecure ones. Of the two secure protocols, the results in Fig. 12 show that the STRS-RZLAR protocol outperforms the SCS-RZLAR in data delivery due to the limitations in the size of the request zone for the SCS-RZLAR (fewer nodes in the zone). Such limitations in the size of the request zone explain the efficiency of the standard-LAR protocol in delivering data packets over the other insecure protocols.

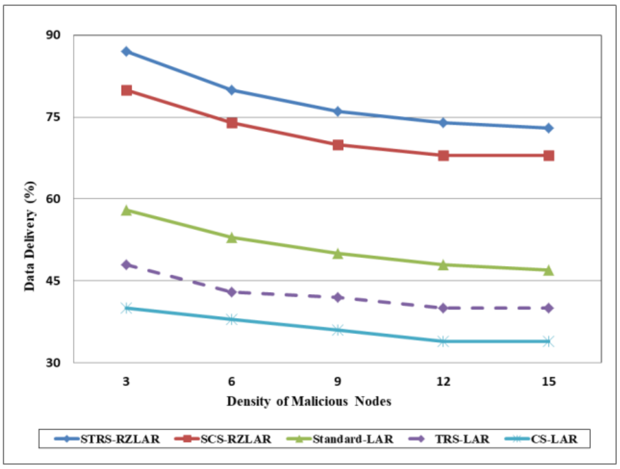

Fig. 12. Effect of MITMAs on data delivery. 60 vehicular nodes; Node speed is 12 m/s

From the other hand, the results in Fig. 13 show the efficiency of using the SCS-RZLAR protocol in minimizing the routing overhead. Such enhancement is due to the improvement in the shape of the SCS-RZLAR request zone that limits the number of RREQ broadcasts to the nodes in such smaller zone (i.e. less routing overhead). Such improvement explains why CS-LAR outperforms all other insecure protocols regarding NRL.

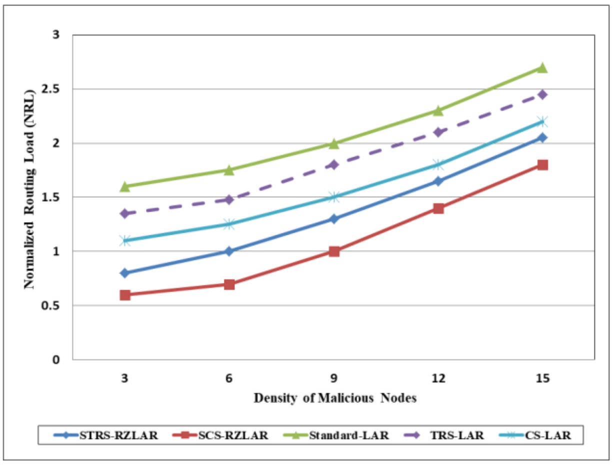

Fig. 13. Effect of MITMAs on NRL. 60 vehicular nodes; Node speed =12 m/s.

The effect of the MITMAs on the average end-to-end packets delay NPM is shown in Fig. 14. Simulation results show that the insecure protocols have less average packets delay than the secure ones and are irrelevant to the number of MITMAs. This is because these protocols do not have any security association phase. From the other side, the results show the negative effect of the number of the MITMAs on the average end-to-end packet delay, where the probability of detecting malicious nodes increases (i.e. more security association overhead). Of the two proposed secure routing protocols, results show that the SCS-RZLAR protocol outperforms the STRS-RZLAR regarding average total packet delay. Such enhancement is due to the improvement in the size of the SCS-RZLAR request zone that limits the number of RREQ broadcasts (i.e. less overhead delays).

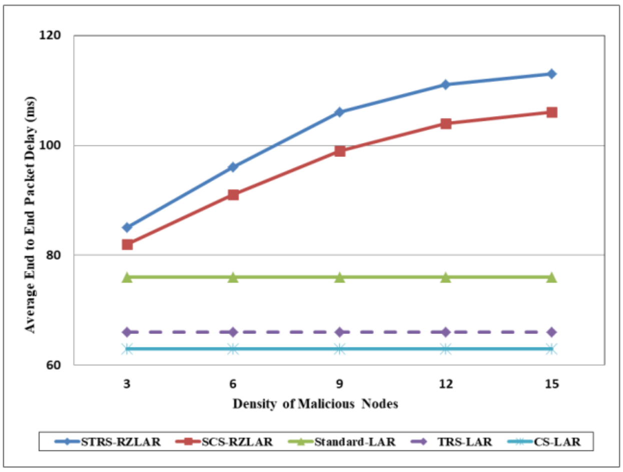

Fig. 14. Effect of MITMAs on average end-to-end packet delay. 60 vehicular nodes; Node speed is 12 m/s.

D. *Speed Effect*

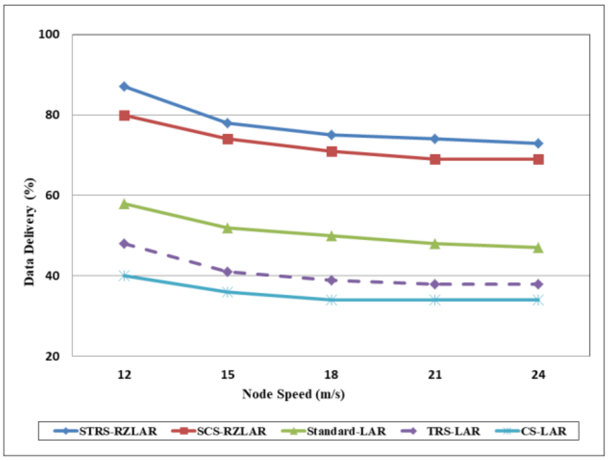

Fig. 15. Effect of node speed on data delivery. 60 vehicular nodes; 10% malicious nodes

The effect of the vehicular node speed on the NPMs was studied over a VANET of 60 vehicular nodes. The percentage of the malicious nodes was set to 10% of the overall nodes (i.e., 6 malicious nodes). The average velocity (v) was varied from 12 m/s to 24 m/s with a step of 3 m/s (i.e. v={12, 15, 18, 21, 24}; α = 3). Simulation results show the negative effect of high node speed on the three NPMs: data delivery, NRL, and average end-to-end packet delay as shown in Fig. 15, Fig. 16, and Fig. 17 respectively. As the speed of the nodes increases, the route breaking increases for all protocols, thereby decreasing the percentage of data delivery to destination as shown in Fig. 15. The results show the enhancement in data delivery through the detection of MITMA by the secure protocols.

The results also show that the STRS-RZLAR protocol outperforms the SCS-RZLAR in data delivery due to the limitations in the size of the request zone for the SCS-RZLAR (fewer nodes in the zone).

Fig. 16 shows that as the speed of the nodes increases, the routing overhead accumulates for all protocols. With higher node speed, the frequency of route breaking increases; thereby increasing the routing overhead (more RREQs to discover new routes) which results in higher values for NRL. the results also show the efficiency of using that the secure routing protocols over the insecure ones in terms of NRL. This is due to the exclusion of the MITMAs from the route to the destination and thus minimizing the number of route disconnections (i.e. less RREQ packets). Of the two secure protocols, the results show that the SCS-RZLAR protocol outperforms the STRS-RZLAR regarding NRL and that's due to the improvement in the shape of the SCS-RZLAR request zone that limits the number of RREQ broadcasts to the nodes in such smaller zone.

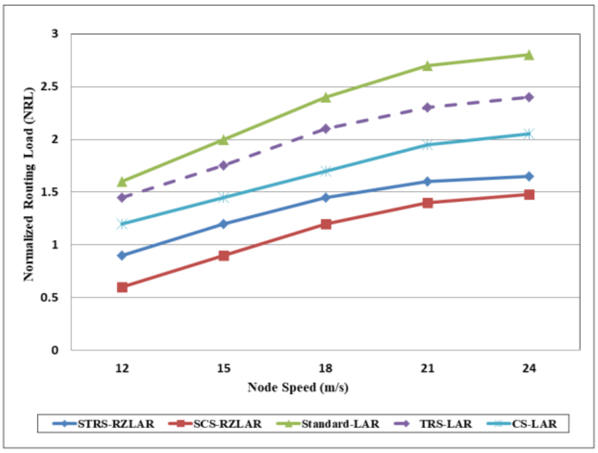

Fig.16. Effect of node speed on NRL. 60 vehicular nodes; 10% malicious nodes

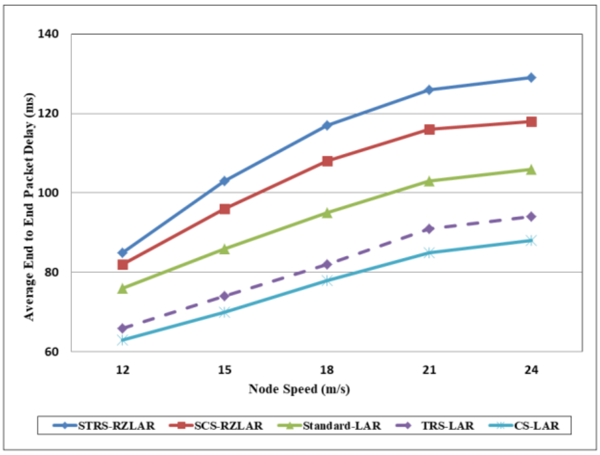

Fig. 17. Effect of node speed on average end-to-end packet delay. 60 vehicular nodes; 10% malicious nodes

The effect of the node speed on the average total packet delay is shown in Fig. 17. The results show the negative effect of using secure protocols on such NPM, where additional overhead from security association phase is added by such secure protocols. The results also show the performance of using the SCS-RZLAR protocol in minimizing such NPM due to the limitation of the number of RREQ broadcasts to such a smaller cone-shaped request zone.

VI. Conclusion

In this work, two optimized secure routing protocol for VANETs were proposed: STRS-RZLAR and SCS-RZLAR protocols. The security unit in both protocols integrates two security agreement protocols: Diffie-Hellman key agreement and a short authentication string (SAS)-based key agreement protocols to provide a robust Wi-Fi based VANET against MITMAs. Extensive Simulations based on QualNet simulator are accomplished to measure different NPMs for VANETs with different network parameters. Simulation results show that the proposed secure protocols improve secure data delivery and NRL with a trade-off in average total packet delay. Of the two secure protocols, results show that SCS-RZLAR protocol outperforms the STRS-RZLAR regarding NRL and average end to end packet delay, while STRS-RZLAR protocol outperforms the SCS-RZLAR in terms of data delivery.

Conflict of Interest

The author declares no conflict of interest.

References

[1] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.

[2] J. Singh and K. Singh, "Congestion control in vehicular ad hoc network: A review," *Next-Generation Networks (Advances in Intelligent Systems and Computing)*, vol. 638, pp. 489-496, 2018.

[3] I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, and N. Guizani, "Overcoming the key challenges to establishing vehicular communication: Is SDN the answer," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 128–134, Jul. 2017.

[4] M. Saleh, "Security aware routing protocol for intelligent transportation distributed multi-agent system," *International Journal of Computer Applications*, vol. 180, no. 10, pp. 5-13, Jan. 2018.

[5] J. Zhao, Y. Wang, H. Lu, Z. Li and X. Ma, "Interference-Based QoS and capacity analysis of VANETs for safety applications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2448-2464, Mar. 2021.

[6] R. A. Nazib and S. Moh, "Routing protocols for unmanned aerial vehicle-aided vehicular ad hoc networks: A survey," *IEEE Access*, vol. 8, pp. 77535-77560, Apr. 2020.

[7] P. Van Mieghem, H. D. Neve, and F. A. Kuipers "Hop-by-Hop quality of service routing," *Computer Networks*, vol. 37, no. 3-4, pp. 407- 423, Nov. 2001.

[8] G. Liu and K. G. Ramakrishnan, "A*Prune: An algorithm for finding K shortest paths subject to multiple constraints,"

Proc. IEEE Twentieth Ann. Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2001), vol. 2, pp. 743-749, 2001.

[9] T. Korkmaz and M. Krunz "Multi-Constrained optimal path selection," in *Proc. IEEE Twentieth Ann. Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2001)*, vol. 2, pp. 834-843, 2001.

[10] L. Rosati, M. Berioli, and G. Reali, "On ant routing algorithms in ad hoc networks with critical connectivity," *Ad Hoc Networks*, vol. 6, no. 6, pp. 827-859, Aug. 2008.

[11] J. Kakarla, S. S. Sathya, B. G. Laxmi, and B. R. Babu, "A survey on routing protocols and its issues in VANET," *IJCA*, vol. 28, no. 4, Aug. 2011.

[12] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao, and C. F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," *IEEE Systems Journal*, vol. 9, no. 1, pp. 65–75, Mar. 2015.

[13] A. K. Sharma and M. C. Trivedi, "Performance comparison of AODV, ZRP and AODVDR routing protocols in MANET," in *Proc. International Conference on Computational Intelligence Communication Technology (CICT)*, Feb. 2016, pp. 231–236.

[14] R. A. Nazib and S. Moh, "Reinforcement learning-based routing protocols for vehicular ad hoc networks: A comparative survey," *IEEE Access*, vol. 9, pp. 27552-27587, Feb. 2021.

[15] G. Sun, Y. Zhang, H. Yu, X. Du and M. Guizani, "Intersection fog-based distributed routing for V2V communication in urban vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 6, pp. 2409-2426, Jun. 2020.

[16] L. R. Gallego-Tercero, R. Menchaca-Mendez, and M. E. Rivero-Angeles, "Efficient time-stable geocast routing in delay-tolerant vehicular ad-hoc networks," *IEEE Access*, vol. 8, pp. 171034-171048, Sept. 2020.

[17] A. Ullah, X. Yao, S. Shaheen, and H. Ning, "Advances in position based routing towards ITS enabled FoG-Oriented VANET–A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 2, pp. 828-840, Feb. 2020.

[18] L. Hu and Z. Dai, "Performance and reliability analysis of prioritized safety messages broadcasting in DSRC with hidden terminals," *IEEE Access*, vol. 8, pp. 177112-177124, Sept. 2020.

[19] E. M. Mohamed, M. A. Abdelghany, and M. Zareei, "An efficient paradigm for multiband WiGig D2D networks," *IEEE Access*, vol. 7, pp. 70032-70045, 2019.

[20] P. Wang, C. Chen, S. Kumari, M. Shojafar, R. Tafazolli, and Y. Liu, "HDMA: Hybrid D2D message authentication scheme for 5G-Enabled VANETs," *IEEE Transactions on Intelligent Transportation System*, Aug. 2020.

[21] O. Sadio, I. Ngom, and C. Lishou, "Controlling WiFi direct group formation for non-critical applications in C-V2X network," *IEEE Access*, vol. 8, pp. 79947-79957, Apr. 2020.

[22] A. Tufail, M. Fraser, A. Hammad, K. K. Hyung, and S. W. Yoo, "An empirical study to analyze the feasibility of WIFI for VANETs," in *Proc. International Conference on Computer Supported Cooperative Work in Design*, pp. 553–558, Apr. 2008.

[23] A. K. Goyal, A. K. Tripathi, and G. Agarwal, "Security Attacks, Requirements and Authentication Schemes in VANET," in *Proc. International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, vol. 1, no. 1, pp. 1-5, 2019.

[24] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," *IEEE Access*, vol. 8, pp. 207308-207342, Nov. 2020.

[25] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A survey on privacy-preserving authentication schemes in VANETs: Attacks, challenges and open issues," *IEEE Access*, vol. 9, pp. 153701-153726, Nov. 2021.

[26] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907–919, 2014.

[27] M. Poongodi, M. Hamdi, A. Sharma, M. Ma, and P. K. Singh, "DDoS detection mechanism using trust-based evaluation system in VANET," *IEEE Access*, vol. 7, pp. 183532-183544, 2019.

[28] A. Sinha and S. K. Mishra, "Preventing VANET from DOS & DDOS attack," *Int. J. Eng. Trends Technol.*, vol. 4, no. 10, pp. 4373–4376, 2013.

[29] K. Verma and H. Hasbullah, "Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET," *Secur. Commun. Netw.*, vol. 8, pp. 864–878, Mar. 2015

[30] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2010, pp. 1–5.

[31] V. Pathak, D. Yao, and L. Iftode, "Securing location aware services over VANET using geographical secure path routing," in *Proc. IEEE International Conference on Vehicular Electronics and Safety*, Sep. 2008, pp. 346–353.

[32] M. Saleh, L. Dong, A. Aljaafreh, and N. Al-Oudat, "Secure location-aided routing protocols with Wi-Fi direct for vehicular ad hoc networks," *Int. Journal of Communication Networks and Information Security*, vol. 12, no. 1, pp. 11-17, 2020.

[33] J. Wang, H. Chen, and Z. Sun, "Context-Aware quantification for VANET security: A markov chain-based scheme," *IEEE Access*, vol. 8, pp. 173618-173626, Aug. 2020.

[34] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular security through reputation and plausibility checks," *IEEE Systems Journal*, vol. 8, no. 2, pp. 384–394, Jun. 2014.

[35] S. A. Alfadhli, S. Lu, K. Chen, and M. Sebai, "MFSPV: A multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs," *IEEE Access*, vol. 8, pp. 142858-142874, 2020.

[36] T. Gazdar, A. Belghith, and H. Abutar, "An enhanced and distributed trust computing protocol for VANETs," *IEEE Access*, vol. 6, pp. 380-392, Oct. 2017.

[37] A. Tolba, "Trust-Based distributed authentication method for collision attack avoidance in VANETs," *IEEE Access*, vol. 6, pp. 62747-3536, Oct. 2018.

[38] M. H. Eiza, T. Owens, and Q. Ni, "Secure and robust multi-constrained QoS aware routing algorithm for VANETS," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, Feb. 2016.

[39] A. Chinnasamy, S. Prakash, and P. Selvakumari, "Enhance trust based routing techniques against sinkhole attack in AODV based VANET," *International Journal of Computer Applications*, vol. 65, no. 15, Mar. 2013.

[40] Y. B. Ko and N. H. Vaidya, "Location-aided routing (lar) in mobile ad hoc networks," *Wireless Networks*, vol. 6, no. 4, pp. 307–321, 2000.

[41] S. M. Senouci and T. M. Rasheed, "Modified location-aided routing protocols for control overhead reduction in mobile ad hoc networks," in *Proc. International Conference on Network Control and Engineering for QoS, Security and Mobility*, Nov. 2005, pp. 137-146.

[42] M. Saleh, "Secure tilted-rectangular-shaped request zone location-aided routing protocol (STRS-RZLAR) for vehicular ad hoc networks," in *Proc. 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2019)*, Nov. 2019, pp. 248-253.

[43] R. Pass, "On deniability in the common reference string and random oracle model," in *Proc. Annual International Cryptology Conference*, Springer, 2003, pp. 316–337.

[44] A. Kumar, S. K. Kaushik, R. Sharma and P. Raj, "Simulators for wireless networks: A comparative study," in *Proc. International Conference on Computing Sciences*, 2012, pp. 338-342.

[45] R. Bagrodia, *et al*., "Parsec: A parallel simulation environment for complex systems," *IEEE Computer Magazine*, vol. 31, no. 10, pp. 77-85, Oct. 1998.

Ma'en Saleh (M'10) received his Ph.D. degree in Electrical and Computer Engineering from Western Michigan University in 2012. He joined the faculty of Tafila Technical University as an Assistant Professor of Electrical and Computer Engineering in 2012. He joined the ECE department at Baylor University, TX in 2016 as a postdoctoral researcher. He promoted to Associate Professor in 2018. His research interests include Real-Time Scheduling for Packet Switched Networks, Security in VANETs, Simulating Real-Time Networks, Real-Time Agent-Based Systems, and QoS for Heterogeneous Networks.