Adaptive Security-aware Cone-shaped Request-zone Location-aided Routing Protocol Using Agent-Based Methodology for VANETs

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

***Abstract*—**In this paper, we propose an agent-based adaptive security-aware enhancement algorithm with congestion control mechanism for limited resources VANETs using intelligent transportation systems. The proposed security algorithm is to be installed at a central server that receives information about the vehicle resources from distributed intelligent road side units (RSUs) in a virtual segmented road via existing wireless cellular networks (4G). The security algorithm adaptively makes a decision about the best integrity security service level a source node can adopt while encrypting its data flows according to a resource estimation congestion control mechanism. The information about the security level decision will be transferred from the central server to the RSU via wireless cellular networks (4G). From the other side, the RSU transfers it to the source vehicle node via Wi-Fi direct technology. In finding the secure route to destination, we adopt our previously proposed secure cone-shaped request-zone LAR (SCSLAR). In order to notify the destination node with the security level that was adopted by the source, we override the 1st 3 bits of the 1st payload byte of the IEEE 802.11 wireless frame format to represent the associated integrity security level. Using three main network parameters: node density, vehicular speed, and number of malicious nodes, extensive simulation results based on QualNet simulator that is based on the GloMoSim used by Scalable Network Technologies (SNT) show that the proposed secure cone-shaped request zone LAR with resource estimation methodology (SCSLAR-RE) outperforms the SCSLAR regarding data delivery and in protecting the VANET from being congested by heavy traffic load through minimizing both the buffer consumption and the average packets delays at the destination side, while providing the best integrity security level to the data streams that make them robust against the alteration threat.

***Index Terms*—**Agents, integrity, VANETs, QoS, security, IoT

I. Introduction

The recent revolution in vehicular communications and internet of things (IoT) played a key role in improving the design process of Intelligent Transportation Systems (ITS) and enhancing their efficiency [1]-[3]. Vehicular Ad-hoc Network (VANET) is the fundamental infrastructure of the ITS that is defined as a heterogeneous, self-organized, and distributed expansion of a mobile ad-hoc network (MANET) with a real-time dynamic communication between its entities [4]-[6] (i.e. vehicle to vehicle communication (V2V) [7] and vehicle to infrastructure communication (V2I) [8], [9]). The hierarchal relationship between IoTs and VANETs is shown in Fig. 1, where VANETs are considered as a subclass of IoTs that adopts various attributes from both IoTs and MANETs [10]. Such relationship allows different types of entities to be connected to the VANET such as electric vehicles (EVs) [11], smart grids [12], charging spots [13], and solar panels resulting in a new network called Internet of energy (IoE) [14].

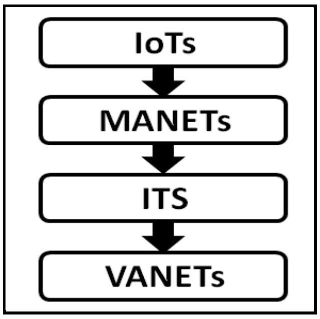

Fig. 1. IoTs and VANETs

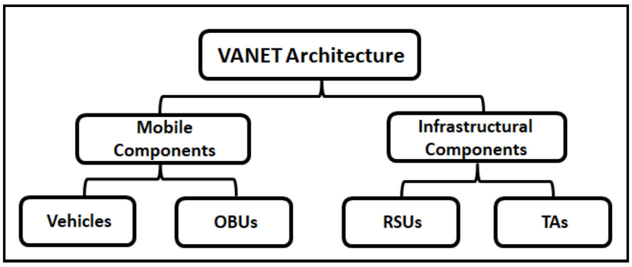

Fig. 2. Architecture of VANETs

A VANET consists of various types of components that are interacting efficiently using different types of communication schemes [15]. Such components belong to two main categories: mobile and infrastructural components. Mobile components include all types of vehicles such as cars, busses, trucks, and EVs [16]. Mobile components also include handheld devices by passengers (i.e. cellular phones and laptops) and On-Board data units (OBU) such as GPS, sensors, communication interfaces and data processors [17], [18]. From the other side, infrastructural components include those components that coordinate the various types of communication schemes inside the VANET such as the road-side units (RSUs) and the centralized trusted authority component (TA) for

Manuscript received August 30, 2021; revised April 18, 2022.
Corresponding author email: van.nguyenngoc@hust.edu.vn.
doi:10.12720/jcm.17.5.308-321

security issues [19]. Such components are part of a distributed system, where each RSU and TA coordinates the communication process in a road segment that is defined by specific dimensions [20]. The component-based architecture of a VANET is shown in Fig. 2.

To provide an efficient and reliable communication between the various components of a VANET (i.e. vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to grid (V2G), and vehicle to everything (V2X)) [21], different communication schemes were adopted such as dedicated short range communication (DSRC) based on the IEEE802.11p standard, Wireless Access in Vehicular Environment (WAVE), WiGig, 3G, 4G, 5G, and LTE cellular networks [22], [23]. In order to solve the limitations of the previous communication schemes (i.e. low channel bandwidth, low data rates, high attenuation, hardware cost, and security issues), Wi-Fi Direct based on the IEEE 802.11n standard was adopted for reliable and secure data communication in high speed VANETs [24], [25].

Various types of services and applications are provided by VANETs including safety applications, comfort applications, commercial applications, and environmental applications [26]-[28]. Due to the nature of wireless networks (i.e. data broadcasting, infrastructure-less model, high-dynamic topology changes, and unpredictable mobility patterns for vehicular nodes) [29], various types of security attacks are launched on the different layers of the VANET and thus degrading the overall security services provided by the VANET which may lead into a catastrophe [30]-[32]. To insure proper services, both quality of service (QoS) and security requirements must be guaranteed.

Accordingly, different secure position-based routing protocols were proposed [33]-[36]. Such protocols use GPS positioning services to minimize the overhead in route calculation and localization and thus provide the best QoS to the customers. From the other side, the security association integrated to such routing protocols provides different types of security services (i.e. confidentiality, integrity, and availability) making the VANET robust against different types of security threats [37], [38].

In this paper, we propose an agent-based adaptive security-aware enhancement algorithm with congestion control mechanism for limited resources VANETs using intelligent transportation systems. The key features of the proposed system are as follows:

1) The proposed system combines the functionality of real-time routing with security services enhancement. The real-time routing uses the cone-shaped LAR routing protocol, while (CSLAR), while the security service enhancement scheme adopts a congestion control mechanism based on resource estimation.
2) The proposed intelligent system was designed using Gaia agent-oriented methodology, where the overall system was decomposed into agents with a well-defined communication protocol governs the interactions between them.
3) The security enhancement unit adaptively makes a decision about the best integrity security service level a source node can adopt while encrypting its data flows according to a resource estimation congestion control mechanism.
4) The congestion control mechanism efficiently utilizes the buffering system at the vehicle queue, hence protecting the network from being congested by heavy traffic loads. From the other side, the queue sub-agent stores the requests collected by the RSUs from the source nodes according to the earliest deadline first algorithm (EDF).
5) In order to notify the destination node with the integrity security level that was adopted by the source, we override the 1st 3 bits of the 1st payload byte of the IEEE 802.11 wireless frame format to represent the associated integrity security level.

The rest of the paper is organized as follows: Section II briefly introduced the related research progresses. The agent-based design model for the proposed system is described in Section III. Section IV presents The Integrity Security Service Design. Section V illustrated the overall system methodology of the proposed system. With extensive simulations, Section V displays the performance evaluation of the proposed system. Finally, conclusions are drawn in Section VI.

II. Related Work

To provide the required security services for VANETs and making them robust against different classes of security threats, various solutions have been proposed with different approaches. In [39], a security model for detection and elimination of malicious nodes in VANETs was proposed. The model is based on electing an observer node with the highest trust value to evaluate the behavior of other nodes in the VANET and classify them as trusted with a specific trust value or malicious node that will be deleted from any routing path to the destination. In [40], an intrusion detection model to evaluate the trustworthiness of a node in a VANET was proposed. According to the nodes behavior during the packet forwarding process, each node updates the trust values of its neighboring nodes based on belief, disbelief, and uncertainty factors. The node then shared such trust values with its neighbors. A malicious node is detected when the disbelief factor exceeds a certain threshold. Accordingly, all nodes will be notified by such node and will be removed from any route to destination.

A secure and QoS aware routing protocol for VANETs was proposed in [41]. The protocol selects the best path to the destination according to the highest confidence level for the path nodes and the minimum message reachable time (MRT).

In [42] A reactive on-demand routing protocol with Cuckoo search algorithm (AODVCS) was proposed for VANETs. The routing protocol was integrated with a trust prediction mechanism and uses the biologically inspired cuckoo search algorithm to select the shortest secure path to the destination.

An improved AODV routing protocol based with genetic simulated annealing, security and stability (GSS-AODV) was proposed for VANETs in [43]. The secure scheme uses both node stability and node trust values to control the path selection process and dynamically adjusts the genetic algorithm parameters such that the resulting path is the most secure and stable one. In [44], an ant colony optimization technique was deployed to propose a secure ant-based multi-constrained quality of service routing protocol (S-AMCQ). The optimization technique selects the best secure route to destination according to the requested QoS constrained by the real-time data flows in a VANET.

A security-aware request-zone LAR (SLAR) routing protocol was proposed in [25] for VANETs. The protocol selects the best secure route to the destination according to a security association phase performed over Wi-Fi direct technology. A Secure tilted-rectangular-shaped request-zone LAR protocol (STRS-RZLAR) for VANETs was proposed in [34]. The security unit integrated to such optimized LAR protocol is based on modified Diffie-Hellman key agreement scheme. The protocol detects the man-in-the-middle attacks (MITMAs) and deletes such malicious nodes from any path to destination. A security-aware roadside routing protocol with resource estimation methodology (SRSR_RE) for VANETs was proposed in [35]. The proposed algorithm was modeled by a distributed multi-agent system and to be installed at each road-side base-unit (RSU). The proposed protocol provides both security and quality-of-service (QoS) requirements as requested by the real-time data flows in a VANET.

Secure cone-shaped request-zone LAR (SCS-RZLAR) for VANETs was proposed in [36]. The integrated security unit to the LAR protocol is a multi-layer unit that adopts two security agreement protocols: modified Diffie-Hellman key agreement protocol and short authentication string (SAS)-based key agreement protocol. Using Wi-Fi Direct out-of-band communication channels, the proposed secure protocol provide a reliable and secure data transmission between VANET components and thus making it robust against MITMAs. A security aware AODV routing protocol for detecting black hole attacks in a VANET was proposed in [45]. The detection process depends on storing all route replies in a lookup table by the source node and assigning them a specific priority number based on their sequence numbers. Accordingly, the source node discards the RREP having presumably very high destination sequence number and thus reducing the effect of black hole attack in ITS. In [46], a key agreement and authentication protocol to satisfy the security requirements for a VANET was proposed. The protocol uses a digital signature mechanism that ensures the privacy of the communication between vehicle nodes and provides a mechanism for immediate emergency reporting.

A trust routing protocol for VANET baptized (TRPV) was proposed in [47]. The protocol uses the trustworthiness of the path and the number of hops in order to find the optimal secure and reliable route to the destination.

A security-aware routing protocol for urban vehicular environment based on trust (TROUVE) was proposed in [48]. The protocol computes the trustworthiness of the whole end-to-end path in order to select the most trusted and shortest route to the destination according to the neighborhood information received by cooperative awareness messages (CAM). A channel state routing protocol (CSRP) for improving the reliability and security of communication schemes in VANET was proposed in [49]. The proposed protocol ensures both QoS and security requirements of the real-time data flows in a VANET by minimizing the energy exploited by On-board units and time delay, while keep enhancing the recognition rate of collision and broadcast rate.

A secure and reliable multi-constrained QoS aware routing protocol (S-AMCQ) was proposed for VANETs in [50]. The protocol deploys the VANET-oriented evolving graph (VoEG) to guarantee the consistency of the authenticated received routing control messages and thus preventing the malicious nodes from being in the selected path to the destination.

III. Agent-Based Design Model

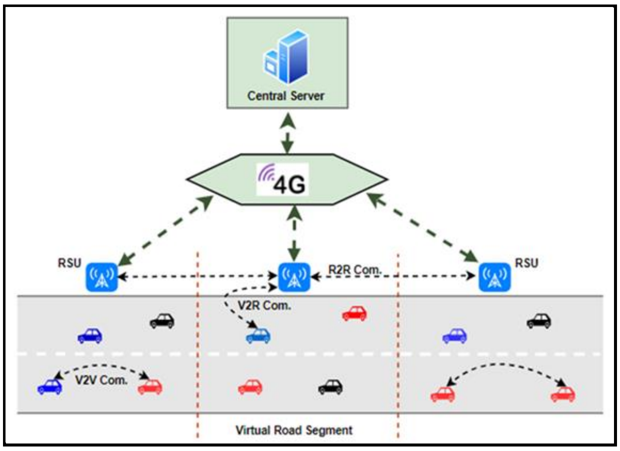

Fig. 3. Intelligent Transportation System (ITS) using virtual road segmentation

The proposed intelligent system was designed using Gaia agent-oriented methodology [51]. It deals with both the macro (network) level and the micro (agent) level aspects of the design. The nature of our proposed system makes the Gaia agent model suitable to be adopted as a design tool, where the system has few numbers of heterogeneous and static-functionality agents. From the other side, the goal of our system is to optimize some quality and security measures with static inter-relationships between system components during run-time. According to the Gaia agent-oriented methodology, three main design phases were defined: decomposition, modeling, and protocol design. In order to deploy the agent-based methodology, the entire road was virtually segmented such that each virtual segment is served by an intelligent road-side unit (RSU) as shown in Fig. 3. According to the decomposition phase, the proposed system was decomposed into three main agents: vehicle node, intelligent RSU, and the central server. The main behaviors and functionalities of each agent were defined in the modeling phase, while the communication and interaction processes between the agents were defined in the protocol design phase.

A. Vehicle Node Agent

This agent represents a vehicle node (*N*) in a VANET with a unique physical address (i.e. plate number). It might be a source node, an intermediate node, or a destination node in a VANET. The source node is a node requesting the intelligent RSU agent about the best integrity security service level that it can be adopted by the source agent such that the network congestion is controlled. The intermediate node models a hop node in the secure route to the destination node during the delivery process. The vehicle to vehicle (V2V) and the vehicle to RSU (V2R) communications are accomplished using Wi-Fi Direct technology. In this research, two main system resources were defined for each vehicle node (N_i): the node processing rate (P_i) and the available memory buffer (B_i).

B. Intelligent RSU Agent

This agent is a modular unit deployed at each virtual road segment. The RSU keeps track of the entire vehicle nodes belonging to the road segment it serves through periodic V2R communication control messages (i.e. every time period $t=T$) and updates its active node list (W) accordingly. It's responsible for collecting the requests from the source vehicle nodes regarding the optimal integrity security service levels to be adopted and pass them to the central server agent using 4G wireless cellular network connections. The intelligent RSU interacts with the destination vehicle node and collects the required system resources information needed to evaluate the best security service to be adopted and pass them to the server agent. It also notifies the source agent by the decision evaluated by the server agent regarding the integrity security service level to be adopted. A layer of communication between adjacent RSUs might be accomplished during the process of locating the destination node (i.e. the source and destination nodes are in different virtual road segments).

C. Central Server Agent

The central server agent represents the core of our intelligent system. It governs system functionalities, defines directions of data flows, and adjusts system parameters to ensure proper services. It consists of two main sub-agents: queue sub-agent and the security unit sub-agent. The queue sub-agent is the one which is responsible for queuing and de-queuing processes. In the queuing process, the queue sub-agent stores the requests collected by the RSUs from the source nodes according to the earliest deadline first algorithm (EDF), that is the request with the highest priority (closer to expire) will be at the top of the queue. In the de-queuing process, the request at the top of the queue will be fetched and sent to the security unit sub-agent to be served. The security unit sub-agent adopts a resource estimation congestion control mechanism. It received the fetched request from the top of the queue and evaluates the best integrity security service level a source node can adopt such that the VANET will not be congested. It interacts with the RSUs notifying them with the decision about the security level to be adapted. The communication between the RSU agent and the central server agent is accomplished via 4G wireless cellular network connections. The agent-based model is shown in Fig. 4.

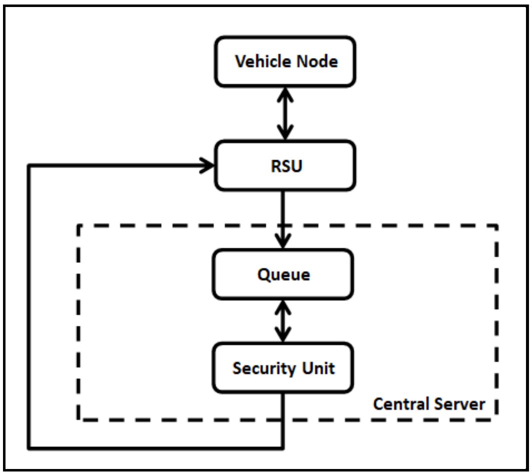

Fig. 4. Agent-based design model

IV. Integrity Security Service Design

In order to combat the alteration threat in the VANET that is the unauthorized attempt to change the data packet's payload, the source node should apply the integrity security service to the data flows. Our proposed system adaptively enhances the security level of the real-time data packets according to the network's status such that the security enhancement should not cause a network congestion that affects the overall network performance metrics (NPMs). In specifying the best integrity security service level to be adopted by the source node, the security unit at the central server adopts a resource estimation methodology for the destination's buffer. Such estimation plays a key role in resolving the network congestion problem. With limited destination buffer resources, heavy traffic load, high integrity security service level, and low processing rate, the chance of dropping packets increases and thus no acknowledgment packets will be sent back to the source node. According to the TCP/IP protocol recovery mechanism, the source node will resend the unacknowledged data packets to the destination which may cause network congestion due to the heavy traffic load in the VANET.

In evaluating the best integrity security service level to be adopted by the source node, the security unit sub-agent at the central server depends on a security overhead model it stores that had been performed for different types of integrity security service algorithms on a 175 MHz–processor machine as shown in Table I [52].

TABLE I: INTEGRITY ALGORITHMS

Security Level (J)	Algorithm	S_j^g	μ_j^g
1	MD4	0.18	46.4
2	MD5	0.26	33.2
3	RIPEMD	0.36	23.3
4	RIPEMD-128	0.45	18.9
5	SHA-1	0.63	13.4
6	RIPEMD-160	0.77	11.1
7	Tiger	1.00	8.5

According to Table I, seven integrity security service algorithms were defined with an associated security level (J). The security level (J) reflects the strength of the algorithm such that the algorithm with the highest security level is the strongest (i.e. Tiger). The efficiency of the security algorithm with a J^{th} security level (S_J^g) is evaluated according to the associated processing rate of the algorithm (μ_J^g) on the 175 MHz– processor machine such that:

$$S_J^g = \frac{8.5}{\mu_J^g} \tag{1}$$

As we can see from Equ.1, there is a trade-off between the security service level and the processing rate of the data, which is the security service algorithm with the highest security level will have the highest security overhead (least processing rate). Accordingly, the status of the buffer resources at the destination side along with traffic rate control the security level to be adopted. With heavy traffic load and limited buffer resources, adopting a high security level may overflow the destination's buffer and thus more dropping for the newly arrived data packets which may cause network congestion due to the packet resending process by the source node.

Since the proposed system adaptively enhances the security level (changing the adopted integrity security algorithm) of the data packets according to the status of the network, a design problem is arises here that is, how would the destination node be notified with the new security algorithm been adopted by the source in order to process the arrived data packets and extract the original payloads?

One design solution is to initiate an offline secure session between the two parties (source and destination) to negotiate and exchange security parameters as in the IPSec protocol, where the parameters exchanged during the security association phase include the security service algorithm, initialization data, encryption data keys, and security modes [53]. Such design solution is not efficient for the our proposed system that adaptively enhances the security service level, where every time we change the security level on the data packets, we have to terminate the secure session and then initiate a new security association session between the two parties to negotiate on the new security parameters which add more security overhead on the network and thus may lead into network congestion.

In order to solve such limitation, our design solution depends on overloading the first three bits ($b_2b_1b_0$) of the first payload byte in the wireless IEEE 802.11 frame format to represent the security level used by the source node [54]. Such overloading allows the identification of eight different integrity security levels (algorithms). The remaining bits (b_4-b_7) are unused for now but could be used when dealing with more integrity security algorithms or when dealing with other security services such as confidentiality and authentication as shown in Fig.5. Upon receiving the data packet by the destination node, it checks such security bits to identify the security algorithm being adopted by the source to be able to process the secured data packet.

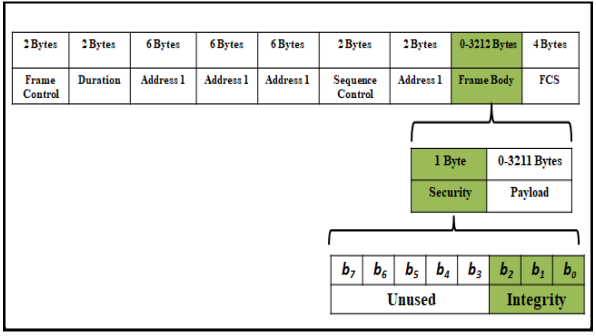

Fig. 5. Overloading the IEEE 802.11 frame format for Integrity Sec. Service

V. SYSTEM METHODOLOGY

The proposed intelligent system adaptively enhances the integrity security service levels of the traffic streams while protecting the overall network from being congested by heavy traffic loads [54]. According to the agent based design model, the process begins upon receiving a request by the intelligent RSU agent from the source agent via Wi-Fi direct communication scheme to serve its data packet flow (f) with the best integrity security service level. The request contains information about the flow average deadline miss ratio (Φ_f), the source address, and the destination address (i.e. plate number). Until being notified with the best security level to be adopted, the source agent starts sending its data packet streams after securing them with the average integrity security service level (J=4), that is the integrity bits ($b_2b_1b_0$) of the first payload byte in the wireless IEEE 802.11packet frame format will be set to 100 indicating the used RIPEMD-128 integrity algorithm by the source. From the other side, the destination node will keep track of two counters: n_f the number of served packets of traffic flow f and t_f is the sum of time differences of packets of traffic f arrived, that is:

$$t_f = \sum_{i=2}^{n_f} (t_i - t_{i-1}) \tag{2}$$

Once the source request received, the RSU agent sends it to the queue sub-agent at the central server agent via 4G wireless cellular network connections. The queue sub-agent checks the average deadline miss ratio (Φ_f) of the received request and queues the request accordingly such that the request with the deadline miss ratio closer to expire will be queued at the top of the queue (EDF). The functionality of the security unit sub-agent at the central server agent is to complete the process of serving the real-time. Once the security unit sub-agent completes serving a current real-time request, in interacts with the queue sub-agent by sending an idle status control message. The queue sub-agent responds to such control message by de-queuing the highest priority request from the top of the queue and passes it to the security unit sub-agent.

Upon receiving the request, the security unit sub-agent broadcasts a control message via 4G wireless cellular network connections to the RSUs requesting the following information: destination counter information (n_f and t_f) and the destination resource information (processing rate (P_f) and size of available buffer (B_f)). Once the message is received by the RSU sub-agent, it checks whether the destination belongs to its segment or not (i.e. destination address$\in W$). If it doesn't, the RSU drops the message. If yes, it interacts with the destination node via Wi-Fi Direct communication scheme requesting for the required information. Once the destination node received the message, it responds with a message (i.e. the destination address is the RSU) including the required information. Upon receiving the message, the RSU sends it back to the security unit sub-agent at the central agent. Once the information is received, the security unit sub-agent calculates the mean inter-arrival time ($\pounds_f$) for the destination's delivered packets of traffic flow f as the following:

$$\pounds_f = \frac{n_f - 1}{t_f} \tag{3}$$

The security unit sub-agent will use such calculated mean inter-arrival time ($\pounds_f$) to determine the buffer size requirements (${Q^j}_f$) needed to enhance n_f real-time packets of flow f using the j^{th} integrity security service level, that is:

$$ {Q^j}_f = \pounds_f * {\boldsymbol{\Upsilon}^j}_f \tag{4}$$

where ${\boldsymbol{\Upsilon}^j}_f$ is the time required to process a packet of length $\mathcal{P}$ using the j^{th} integrity security service level that is:

$$ {\boldsymbol{\Upsilon}^j}_f = \frac{\mathcal{P} * 175MHz}{\mu^J_f * P_f} \tag{5}$$

where (μ^J_f) is the associated processing rate of the j^{th} integrity security service level performed on the 175 MHz processor machine, while P_f *is* the destination's processing rate.

Given the size of destination's available buffer as B_f, the security unit sub-agent makes a decision on the best integrity security service level (r) to be adopted by the source node without congesting the overall VANET, such that:

$$ {Q^r}_f \leq B_f < {Q^{r+1}}_f \tag{6}$$

If the decision on the security level doesn't equal to the initial security level adopted by the source (i.e. $r \neq 4$), then the security unit sub-agent broadcasts a message to the RSUs with the new security level (r) to be adopted by the source node. It also sends an idle status control message to the queue sub-agent. Upon receiving the message on the updated security level, each RSU checks its active node list (W). If the address of the source node doesn't belong to it, the RSU drops the message. Otherwise, the RSU forwards the message to the source node notifying it to modify (enhance/reduce) the security service level to the new value (r). No notification will be sent to RSUs if the decision on the security level equals to the initial security level adopted by the source (i.e. $r = 4$).

Once the source node receives the message regarding the new security level to be adopted, it starts applying the integrity security service algorithm associated to such level as shown in table.1 on its data packets flow and filling the integrity bits ($b_2b_1b_0$) of the first payload byte of each packet with the new security level value (r) . The overall communication protocol between the agent entities in the multi-agent system is shown in Fig. 6.

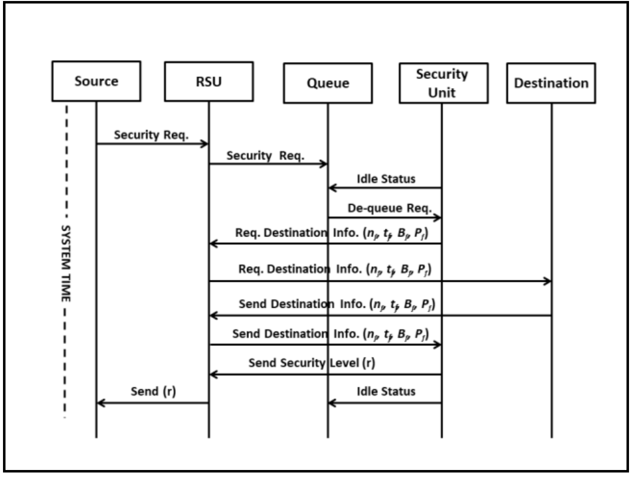
Source
RSU
Queue
Security Unit
Destination
SYSTEM TIME
Security Req.
Security Req.
Idle Status
De-queue Req.
Req. Destination Info. (n_f, t_f, B_f, P_f)
Req. Destination Info. (n_f, t_f, B_f, P_f)
Send Destination Info. (n_f, t_f, B_f, P_f)
Send Destination Info. (n_f, t_f, B_f, P_f)
Send Security Level (r)
Send (r)
Idle Status

Fig. 6. Communication protocol

In order to implement a secure communication scheme between the vehicular nodes in the VANET, we have used our proposed Secure Cone-Shaped Request Zone LAR (SCS-RZLAR) Protocol [36], where a multi-layer security unit that adopts two security agreement protocols was integrated to a Cone-Shaped Request Zone LAR. The first layer adopts the modified Diffie-Hellman key agreement protocol that allows any two nodes with no prior knowledge of each other to establish a shared secret public key using their non-shared private keys (k) along with the Diffie-Hellman common integer parameters (ex. prime modulus (m) and the base (b)). The other layer adopts a short authentication string (SAS)-based key agreement protocol which utilizes a cryptography commitment scheme that is constructed by the use of cryptographic hash functions in the security association phase as a pre-step before generating the shared security keys. Such security association process will be used to detect and exclude the malicious (MITMA) nodes from the route to the destination. It will be implemented over a secure out-of-band channel between a pair of intercommunicated vehicle nodes via Wi-Fi Direct technology. The overall process is described in Fig. 7 [36].

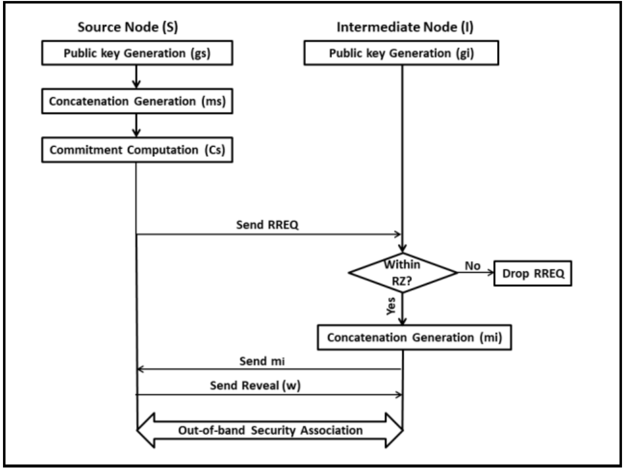
Source Node (S)
Intermediate Node (I)
Public key Generation (gs)
Public key Generation (gi)
Concatenation Generation (ms)
Commitment Computation (Cs)
Send RREQ
Within RZ?
No
Drop RREQ
Yes
Concatenation Generation (mi)
Send mi
Send Reveal (w)
Out-of-band Security Association

Fig. 7. Security agreement process in SCS-RZLAR

Such integration provides a reliable and secure data transmission between vehicle nodes in the VANET with superior performance in minimizing the normalized routing load (NRL) and the average end to end packet delay due to the improvement in the shape of the request zone that limits the number of RREQ broadcasts to the nodes in such smaller zone compared to other request zone shapes as shown in Fig. 8.

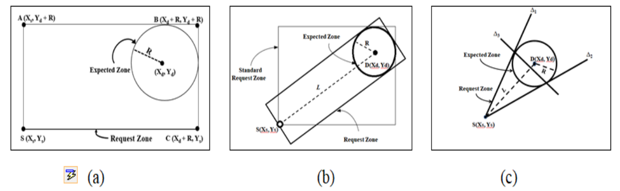

Fig. 8. Request zone shapes: (a) Rectangular; (b) Tilted rectangular; (c) Cone

VI. Simulation & Results

The performance evaluation of our proposed algorithm was performed through simulations. Nevertheless, the parameters and the data needed to drive the network simulator are generated through experiments (i.e. the integrity security overhead model at the security unit sub-agent is based on experimental results of a 175 MHz-processor machine [52] as shown in Table I). Due to the complexity of our heterogeneous environment, that is a dynamic real-time VANET with QoS guarantees and security aspects, conventional network simulators are not sufficient for measuring the network performance metrics (NPMs). Since our model is a multi-agent based scheme with its core sub-agent is a software based agent (i.e. security unit), the simulation model was implemented based on QualNet simulator that is based on the GloMoSim used by Scalable Network Technologies (SNT) [55]. It's a planning, testing, and object-oriented tool that provides a mechanism to inherit the methodologies used to design, optimize and analyze the interactions between the sub-agents. It also allows the agents to synchronize with discrete time-critical events.

A. System Parameter, Assumptions, and Motion Model

In our simulations, the vehicle node and data flow parameters were set as shown in Table II, while the motion model used for the vehicular nodes in the VANET along with the system assumptions is described in Table III.

TABLE II: Vehicle Node & Data Flow Parameters

Parameter	Value
Vehicle sending rate (λ_f)	150 packets/sec.
Vehicle available memory buffer (B_i)	λ_f /10, λ_f /5 multiplied by unit time, or unbounded
Vehicle processing rate (P_f)	175 MHz
Packet length ($\mathcal{P}$)	1500 bytes (max. Ethernet payload)
Flow mean inter-arrival time	1/ λ_f
Flow average deadline miss ratio (Φ_f)	Random variable uniformly distributed on [40ms, 300ms]
Channel rate according to IEEE 802.11.	2 Mbps
Vehicle Diffie-Hellman parameters (modulus (m) and base (b)	Randomly chosen
Vehicle private key (k)	Randomly chosen
Initial Integrity Sec. Service Level (r)	4 (RIPEMD-128 algorithm)

TABLE III: Motion Model & System Assumptions

Parameter/Assumption	Value
Area Dimensions	A square region [1000 m x 1000 m].
Type of movement	Continuous
Average velocity for the nodes (v)	Random chosen between [4 m/s and 30 m/s].
Velocity factor (α)	2 m/s when v<10; 3 m/s when v≥10
The actual speed of the vehicles	Uniformly distributed between [v- α, v+ α]
Vehicle distance per movement (d)	exponentially distributed with a mean of 20 m.
Vehicle Transmission range	200 m
Number of virtual segments	5 segments
Initial location for the vehicle (X_0, Y_0).	Random variable uniformly distributed on [1000m, 1000m]
Source and destination nodes	Randomly selected

B. Node Density Effect

In order to demonstrate the effect of the node density parameter on the overall network performance metrics (NPMs), we simulate a real-time VANET by choosing the number of vehicle nodes N to be {20, 40, 60, 80, and 100}. For each simulation run, the percentage of the malicious nodes was set to be 10 of the node density (N). 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). Fig. 7. shows the effect of the node density on the steady state integrity security service level (r) using different vehicles buffer sizes (i.e.

B= {λ_f /10, λ_f /5, and unbounded}). The integrity security level is higher for destinations with higher buffer sizes (B), where destinations will be more flexible in processing high-security level packets without much caring about being congested by the arrived data packets.

The results in Fig. 9 also show the effect of the node density on enhancing the integrity security level, where networks with high node density increases the normalized routing load (more routing overhead) due to the high node density in the request zone (i.e. more RREQ broadcasts). Such increasing in the normalized routing load (NRL) will have a negative effect on the packets arrival rate at the destination's buffer as shown in Fig. 10 and thus, higher integrity security service level could be adopted.

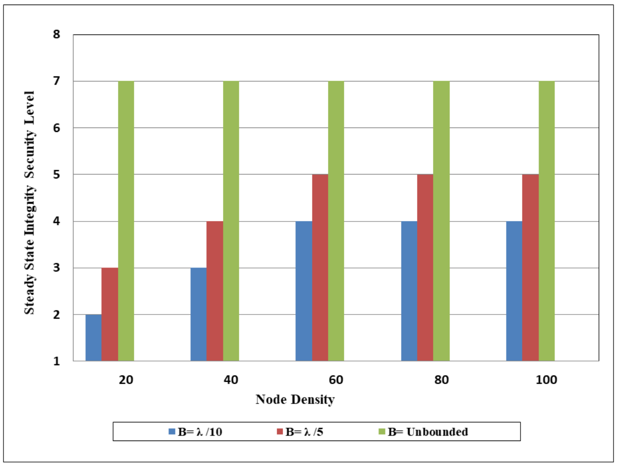

Fig. 9. Average steady state integrity security level

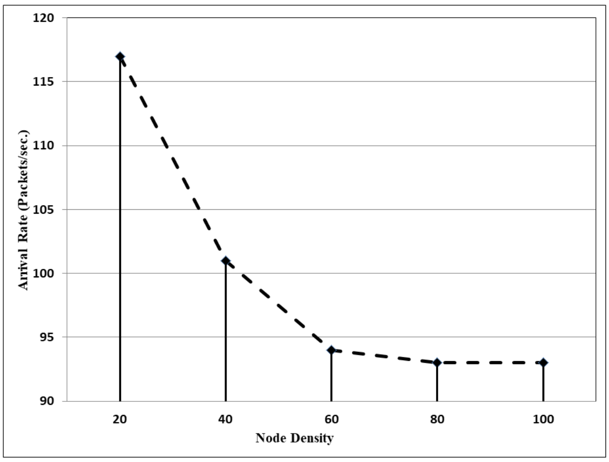

Fig. 10. Packet's arrival rate at destination

In order to measure the effect of the node density on the average data delivery of packets at destination, the proposed adaptive protocol (SCSLAR-RE) was compared with the SCSLAR protocol at the steady-state integrity security level achieved in Fig. 9 for two initial buffer sizes (λ_f /10 and λ_f /5). Fig. 11 shows the positive effect of the node density on the data delivery for the two protocols, where high node density increases the probability of finding a route to destination (i.e. less route disconnections).

The simulation results also show that the proposed protocol outperforms the SCSLAR in data delivery, where the proposed protocol adaptively enhances/decreases the security level of the packets such that the destination's buffer will not be congested, that is newly arrived packets will not be dropped and will be served within the required QoS requirements (i.e. Flow average deadline miss ratio (Φ_f)). As a result, the overall secure data delivery will be enhanced in comparison with the SCSLAR that may congest the destination's buffer by being stuck at the high integrity security level adopted as shown in Fig. 12, where the destination's buffer consumption was measured for the two protocols for the two initial buffer sizes (λ_f /10 and λ_f /5) and by using the steady-state integrity security level for the SCSLAR protocol.

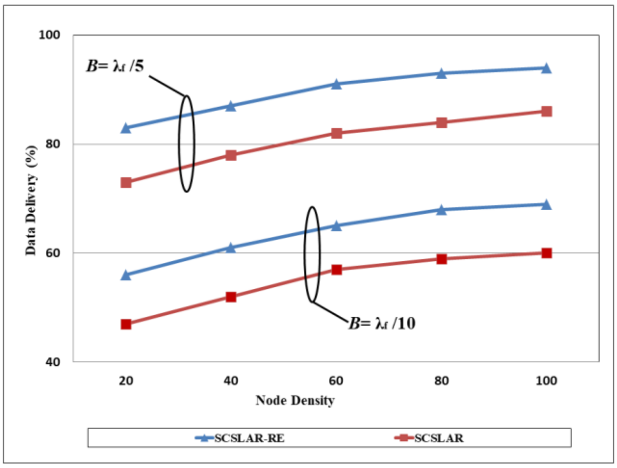

Fig. 11. Effect of node density on data delivery. 10% malicious nodes; 12 m/s node speed.

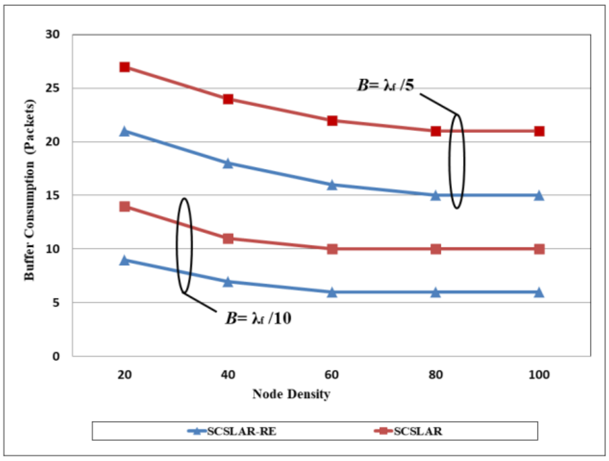

Fig. 12. Effect of node density on data Buffer Consumption. 10% malicious nodes; 12 m/s node speed.

The last network performance metric (NPM) to be measured is the average total packet delay at the destination's buffer. In Fig. 13, the proposed adaptive protocol (SCSLAR-RE) was compared with the SCSLAR protocol at the steady-state integrity security level achieved in Fig. 7 for two initial buffer sizes (λ_f /10 and λ_f /5). The simulation results show that the proposed SCSLAR-RE protocol outperforms the SCSLAR protocol in minimizing the average total packet delay, where being stuck at higher steady state security-level by the SCSLAR protocol will force the destination node to spend high processing time on such highly-secured data packets and thus more waiting time for those queued packets at the destination's buffer. The result also shows that the average packet delays at the destination side is higher for networks with high node densities due to the higher values of data packets delivery for such networks.

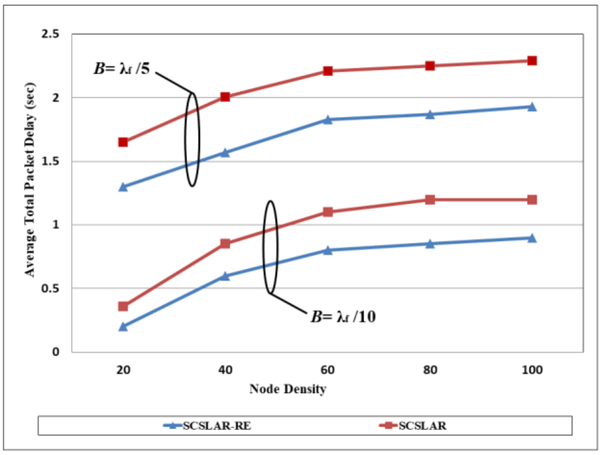

Fig. 13. Effect of node density on average total packet delay. 10% malicious nodes; 12 m/s node speed.

C. Node Speed Effect

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). Fig. 14. shows the effect of the vehicular node speed on the steady state integrity security service level (r) using different vehicles buffer sizes (i.e. B= {λ_f /10, λ_f /5, and unbounded}).

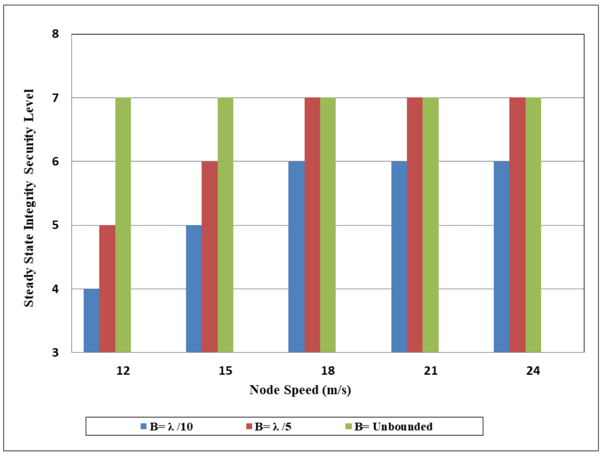

Fig. 14. Average steady state integrity security level

As shown from the simulation result, the integrity security level will be enhanced for higher vehicular node speed values. With higher node speed values, the frequency of route breaking increases; thereby increasing the routing overhead (more RREQs to discover new routes) which results in low packets arrival rate at the destination's buffer as shown in Fig. 15 and thus, higher integrity security service level could be adopted.

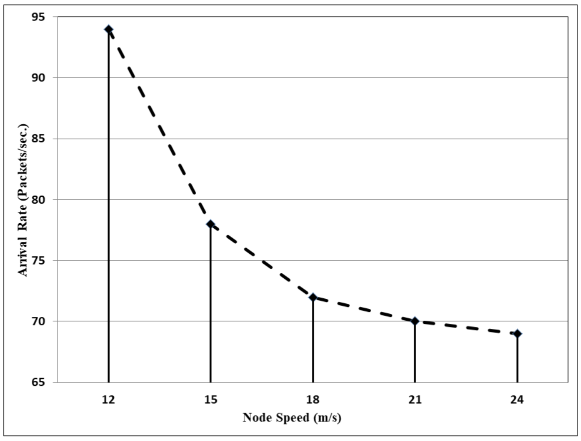

Fig. 15. Packet's arrival rate at destination

The result also shows that the integrity security level is higher for destinations with higher buffer sizes (B), where destinations will be more flexible in processing high-security level packets with lower probabilities of congesting its memory buffer with new arrived data packets.

The effect of the vehicular node speed on the average data delivery of packets at the destination was reflected in Fig. 16, where the proposed adaptive protocol (SCSLAR-RE) was compared to the SCSLAR protocol at the steady-state integrity security level for two initial buffer sizes (λ_f /10 and λ_f /5).

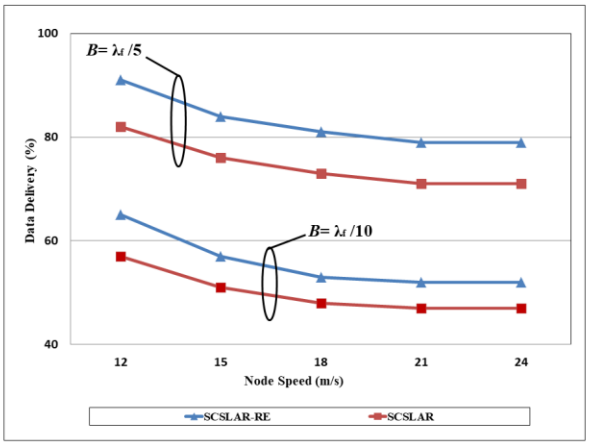

Fig. 16. Effect of node speed on data delivery. 10% malicious nodes; 60 vehicular nodes.

The results show the negative effect of the vehicular node speed on the data delivery for the two protocols. As the speed of the nodes increases, the route breaking increases, thereby decreasing the percentage of data delivery to the destination. Among the two protocols, the results show that the proposed protocol outperforms the SCSLAR in data delivery due to the resource estimation methodology that adaptively modifies the security level such that no congestion occurs at the destination's buffer side.

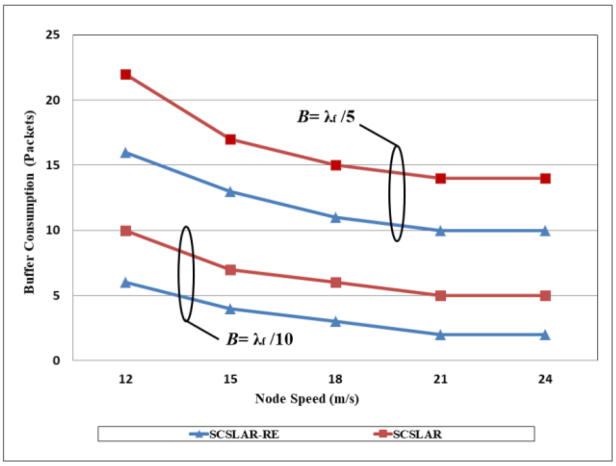

Fig. 17. Effect of node speed on data Buffer Consumption. 10% malicious nodes; 60 vehicular nodes.

The effect of such congestion control adopted by the proposed protocol on the destination's buffer is shown in Fig. 17, where the destination's buffer consumption was measured for the two protocols at different vehicular speeds using the two initial buffer sizes (λ_f /10 and λ_f /5). By using the steady-state integrity security level for the SCSLAR protocol, the simulation result shows that the proposed protocol outperforms the SCSLAR in protecting the destination's buffer from being congested and thus guaranteeing the QoS requirements of the real-time data flows.

In order to measure the effect of the vehicular node speed on the average total packet delays at the destination's buffer, the proposed adaptive protocol (SCSLAR-RE) was compared with the SCSLAR protocol at the steady-state integrity security level achieved in Fig. 14 for the two initial buffer sizes (λ_f /10 and λ_f /5).

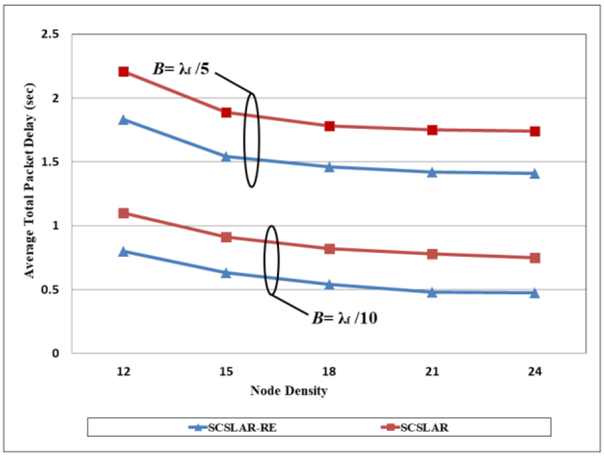

Fig. 18. Effect of node speed on average total packet delay. 10% malicious nodes; 60 vehicular nodes.

The simulation result in Fig. 18 shows that the proposed SCSLAR-RE protocol outperforms the SCSLAR protocol in minimizing the average total packet delay due to the high processing time spent on the data packets that had been secured with a fixed high security level (i.e. the steady state security level) and thus more waiting time for those queued packets at the destination's buffer.

The result also shows that the average packet delays at the destination side is lower for networks with high vehicular node speeds due to the negative effect of high vehicular node speeds on the packets delivery as shown before in Fig. 16.

D. Malicious Nodes Effect

In this section, we studied the effect of the malicious nodes on the network performance metrics including the data delivery, buffer consumption, and average total packet delays at the destination.

In order to do that, extensive simulations were performed over a VANET of 60 vehicular nodes by varying the number of malicious nodes from 10% to 30% of the total number of vehicular nodes with a step of 5% (i.e. malicious nodes = { 6, 9, 12, 15, 18}). 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).

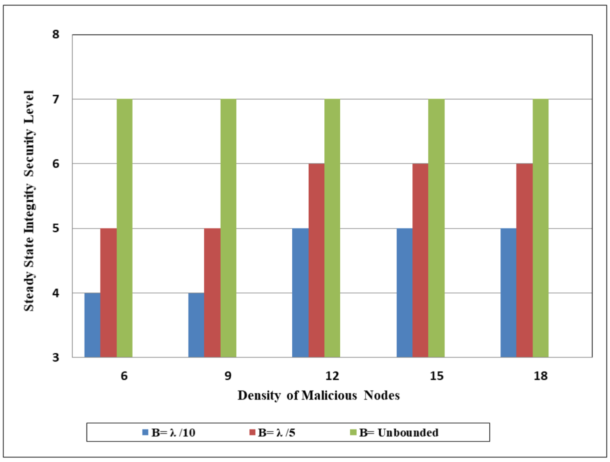

Fig. 19. Average steady state integrity security level

Fig. 19. shows the effect of the density of malicious nodes on the steady state integrity security service level (r) using different vehicles buffer sizes (i.e. B= {λ_f /10, λ_f /5, and unbounded}).

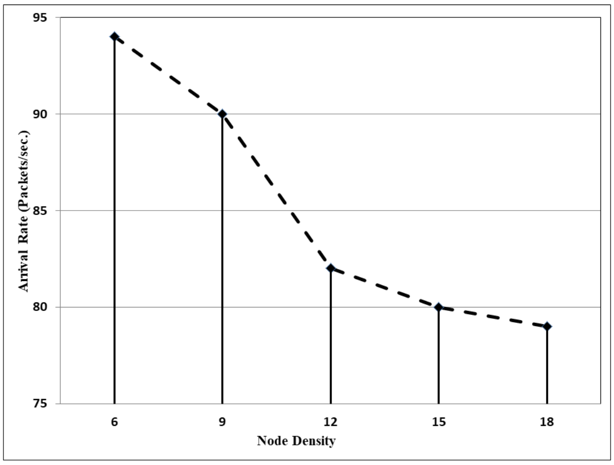

Fig. 20. Packet's arrival rate at destination

The integrity security level will be enhanced for networks with higher densities of malicious nodes, where more security association overhead is added to find a secure route to destination (i.e. more RREQs to discover new routes after excluding the malicious nodes). Such security association overhead will have a negative effect on the packets arrival rate at the destination's side as shown in Fig. 20, and thus more flexibility in adopting a higher security level. Among the different sizes of initial buffers, the results show the possibility of adopting a higher integrity security level for destinations with higher initial buffer size due to the lower probabilities of congesting its memory buffer by the new arrived data packets.

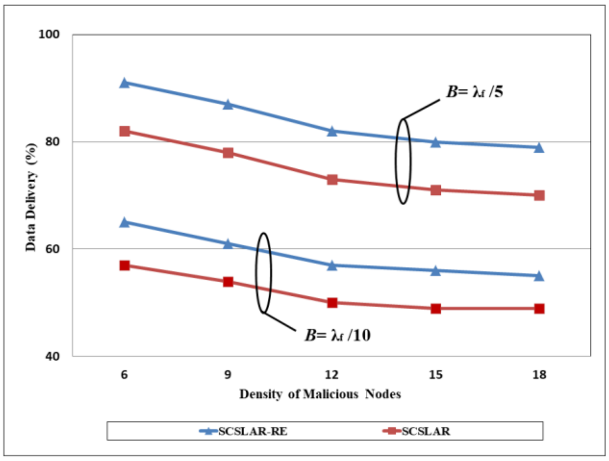

Fig. 21. Effect of malicious nodes on data delivery. 12 m/s node speed; 60 vehicular nodes.

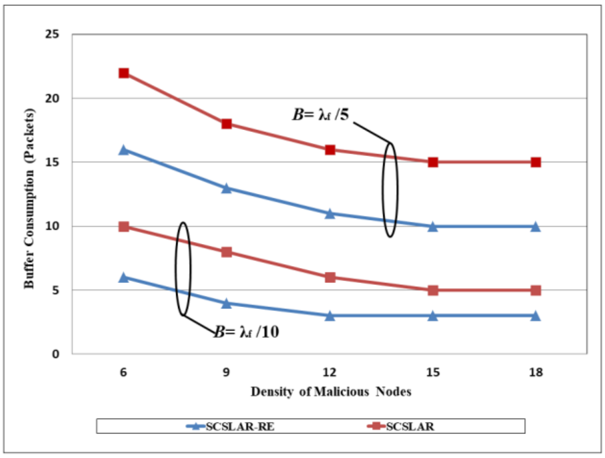

Fig. 22. Effect of malicious nodes on data buffer consumption. 12 m/s node speed; 60 vehicular nodes.

In order to measure the effect of the malicious node density on the average data delivery and the destination's buffer consumption, the proposed adaptive protocol (SCSLAR-RE) was compared to the SCSLAR protocol at the steady-state integrity security level for two initial buffer sizes (λ_f /10 and λ_f /5). Fig. 21 and Fig. 22 show the negative effect of the density of malicious nodes on the two NPMs (i.e. malicious node density on the average data delivery) respectively. The highest the density of the malicious nodes, the highest the security association overhead needed to find a secure route to the destination and thus, the lowest the data delivery and the destination's buffer consumption is.

Among the two protocols, the results in Fig. 21 and Fig. 22 show that the proposed protocol outperforms the SCSLAR regarding the two previous NPMs (i.e. malicious node density on the average data delivery) respectively. Such enhancement is due to the resource estimation methodology adopted by the proposed protocol that adaptively modifies the security levels of the data packet flows to protect the destination from being congested by heavy traffic load while guaranteeing the security and QoS requirements for the data flows.

To study the effect of the density of malicious nodes on the average data packet delays at the destination, the proposed adaptive protocol (SCSLAR-RE) was compared with the SCSLAR protocol at the steady-state integrity security level achieved in Fig. 19 for the two initial buffer sizes (λ_f /10 and λ_f /5). The simulation result in Fig. 23 shows that the proposed SCSLAR-RE protocol outperforms the SCSLAR protocol in minimizing the average total packet delay due high security overhead needed to process the data packets when using the steady state security level by SCSLAR protocol regardless the status of the network, and thus more waiting time the queued packets at the destination's buffer. The results also show that the highest the density of the malicious nodes, the lowest the average total packet delays at the destination side. Such result is due to the negative effect of high density of malicious nodes on the packets delivery at the destination side as shown before in Fig. 19.

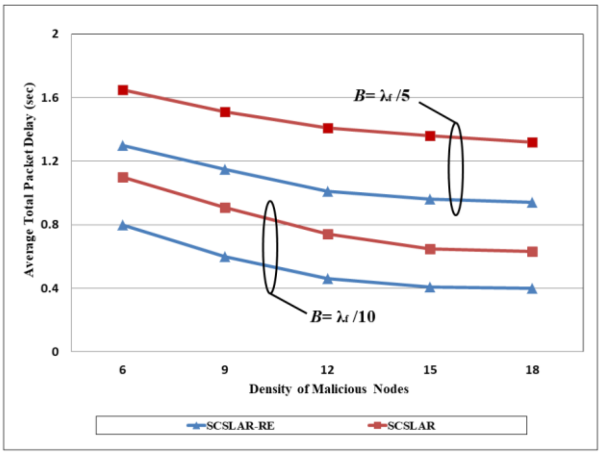

Fig. 23. Effect of malicious nodes on average total packet delay. 12 m/s node speed; 60 vehicular nodes.

VII. Conclusion

In this research, a layer of cooperation is achieved between a real-time routing module and a security enhancement module for limited resources VANET. The overall system is designed and modeled using agent-based methodology such that the integrity security service level adopted by the source vehicle node will be adaptively modified according to a resource estimation congestion mechanism that protects the overall VANET from being congested by heavy traffic load. Extensive simulation results show that our proposed protocol outperforms other security-aware routing protocols regarding different QoS metrics (i.e. data delivery, buffer consumption, and average packet delays), while keeps providing the real-time traffics with the optimized integrity security level needed to combat the effect of alteration security threat in a VANET.

The future work includes performing the security enhancement for different types of security services such as confidentiality and authentication, and thus making the VANET robust against more types of security threats besides the alteration one.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

The proposed system combines the functionality of real-time routing with security services enhancement. The real-time routing uses the cone-shaped LAR routing protocol, while (CSLAR), while the security service enhancement scheme adopts a congestion control mechanism based on resource estimation.

The proposed intelligent system was designed using Gaia agent-oriented methodology, where the overall system was decomposed into agents with a well-defined communication protocol governs the interactions between them.

The security enhancement unit adaptively makes a decision about the best integrity security service level a source node can adopt while encrypting its data flows according to a resource estimation congestion control mechanism.

The congestion control mechanism efficiently utilizes the buffering system at the vehicle queue, hence protecting the network from being congested by heavy traffic loads. From the other side, the queue sub-agent stores the requests collected by the RSUs from the source nodes according to the earliest deadline first algorithm (EDF).

In order to notify the destination node with the integrity security level that was adopted by the source, we override the 1st 3 bits of the 1st payload byte of the IEEE 802.11 wireless frame format to represent the associated integrity security level.

References

[1] B. H. Khudayer, M. Anbar, S. M. Hanshi, and T. C. Wan, “Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks,” *IEEE Access*, vol. 8, pp. 24019–24032, Jan. 2020.

[2] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, and Y. Wang, “A survey of internet of things communication using ICN: A use case perspective,” *Computer Communications*, vol. 142, pp. 95-123, Jun. 2019.

[3] I. Ali, M. Faisal, and S. Abbas, “A survey on lightweight authentication schemes in vertical handoff,” *Int. J. Cooperat. Inf. Syst.*, vol. 26, no. 1, pp. 1-18. Mar. 2017.

[4] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, “A comprehensive review of authentication schemes in vehicular ad-hoc network,” *IEEE Access*, vol. 9, pp. 31309-31321, Feb. 2021.

[5] S. Olariu, “A survey of vehicular cloud research: Trends, applications and challenges,” *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2648–2663, Jun. 2020.

[6] 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.

[7] M. Alzubaidi, M. Anbar, Y. W. Chong, and S. Al-Sarawi, “Hybrid monitoring technique for detecting abnormal behaviour in RPL-based network,” *J. Commun.*, vol. 10, pp. 198–208, Oct. 2018.

[8] G. Singh, “Video streaming communication over VANET,” in *Recent Advances in Computational Intelligence*, Cham, Switzerland: Springer, 2019, pp. 189–197.

[9] 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.

[10] I. U. Din, B. Ahmad, A. Almogren, H. Almajed, I. Mohiuddin, and J. J. P. C. Rodrigues, “Left-Right-Front caching strategy for vehicular networks in ICN-Based internet of things,” *IEEE Access*, vol. 9, pp. 595-605, Dec. 2020.

[11] G. Sun, M. Yu, D. Liao, and V. Chang, “Analytical exploration of energy savings for parked vehicles to enhance VANET connectivity,” *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1749–1761, May 2019.

[12] G. Li, X. Li, Q. Sun, L. Boukhatem, and J. Wu, “An effective MEC sustained charging data transmission algorithm in VANET-Based smart grids,” *IEEE Access*, vol. 8, pp. 101946-101962, May 2020.

[13] G. Sun, M. Yu, D. Liao, and V. Chang, “Analytical exploration of energy savings for parked vehicles to enhance VANET connectivity,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1749-1761, May 2019.

[14] S. Li, F. Wang, J. Gaber, and X. Chang, “Throughput and energy efficiency of cooperative ARQ strategies for VANETs based on hybrid vehicle communication mode,” *IEEE Access*, vol. 8, pp. 114287-114304, Jun. 2020.

[15] X. Chen and L. Wang, “A cloud-based trust management framework for vehicular social networks,” *IEEE Access*, vol. 8, pp. 2967–2980, Feb. 2017.

[16] G. Li, Q. Sun, L. Boukhatem, J. Wu, and J. Yang, “Intelligent vehicle-to-vehicle charging navigation for mobile electric vehicles via VANET-Based communication,” *IEEE Access*, vol. 7, pp. 170888-170906, Nov. 2019.

[17] J. Cui, W. Xu, Y. Han, J. Zhang, and H. Zhong, “Secure mutual authentication with privacy preservation in

vehicular ad hoc networks," *Veh. Commun.*, vol. 21, Jan. 2020.

[18] A. Amjid, A. Khan, and M. A. Shah, "Vanet-based volunteer computing (vbvc): A computational paradigm for future autonomous vehicles," *IEEE Access*, vol. 8, pp. 71763-71774, 2020.

[19] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, and S. M. Hanshi, "Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks," *IEEE Access*, vol. 8, pp. 144957-144968, Aug. 2020.

[20] Z. Wei, J. Li, X. Wang, and C. Gao, "A lightweight privacy-preserving protocol for VANETs based on secure outsourcing computing," *IEEE Access*, vol. 7, pp. 62785-62793, May 2019.

[21] G. Luo, *et al*., "Software-Defined cooperative data sharing in edge computing assisted 5G-VANET," *IEEE Transactions on Mobile Computing*, vol. 20, no. 3, pp. 1212-1229, Mar. 2021.

[22] S. Benkirane and M. Benaziz, "Performance evaluation of IEEE 802.11p and IEEE 802.16e for vehicular ad hoc networks using simulation tools," in *Proc. IEEE 5th International Congress on Information Science and Technology (CiSt)*, Dec. 2018, pp. 573-577.

[23] M. Noor-A-Rahim, G. G. M. N. Ali, Y. L. Guan, B. Ayalew, P. H. J. Chong, and D. Pesch, "Broadcast performance analysis and improvements of the LTE-V2V autonomous mode at road intersection," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 9359-9369, Oct. 2019

[24] 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*, Apr. 2008, pp. 553–558.

[25] 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, Apr. 2020.

[26] S. Olariu, "A survey of vehicular cloud research: Trends, applications and challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2648–2663, Jun. 2020.

[27] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, "An efficient and provably secure ECC-Based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1278-1291, Feb. 2021.

[28] Y. Zhang, L. Zhang, D. Ni, K. K. R. Choo, and B. Kang, "Secure, robust and flexible cooperative downloading scheme for highway VANETs," *IEEE Access*, vol. 9, pp. 5199-5211, 2021.

[29] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028-91047, May 2020.

[30] J. Weng, *et al*., "Benbi: Scalable and dynamic access control on the northbound interface of sdn-based vanet," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 822-831, 2018.

[31] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Trans. Inf. Forensics Security*, vol. 15, no. 1, pp. 1654–1667, Oct. 2019.

[32] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Veh. Commun.*, vol. 16, pp. 45–61, Apr. 2019.

[33] A. R. Deshmukh, P. Nirmal, and S. S. Dorle, "A new approach for position based routing protocols based on Ant Colony Optimization (ACO) technique in vehicular ad hoc network (VANET)," in *Proc. International Conference on Intelligent Technologies (CONIT)*, 2021, pp. 1-5.

[34] M. Saleh, "Secure tilted-rectangular-shaped request zone location-aided routing protocol (STRS-RZLAR) for vehicular ad hoc networks," *Procedia Computer Science*, vol. 160, pp. 248-253, Nov. 2019.

[35] 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.

[36] M. Saleh, "Secure optimized request zone location-aided routing protocols with Wi-Fi direct for vehicular ad hoc networks," *Journal of Communications*, vol. 17, no. 3, 2021.

[37] 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.

[38] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314-54344, 2020.

[39] K. N. Tripathi and S. C. Sharma, "A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS)," *International Journal of System Assurance Engineering and Management*, vol. 11, no.2, pp. 426–440, 2020.

[40] B. Sen, M. G. Meitei, K. Sharma, M. K. Ghose, and S. Sinha, "Mitigating black hole attacks in MANETs using a trust-based threshold mechanism," *International Journal of Applied Engineering Research*, vol. 13, no. 7, pp. 5458–5463, 2018.

[41] M. J. Sataraddi and M. S. Kakkasageri, "Trust and delay based routing for VANETs," in *Proc. IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2019, pp. 1–6.

[42] A. Kout, S. Labed, S. Chikhi, *et al*., "AODVCS, a new bioinspired routing protocol based on cuckoo search algorithm for mobile ad hoc networks," *Wirel Netw*, vol. 9, pp. 1–11, 2017.

[43] J. Mo, B. Huang, X. Cheng, C. Huang, and F. Wei, "Improving security and stability of ad hoc on-demand distance vector with fuzzy neural network in vehicular ad

hoc network," *International Journal of Distributed Sensor Networks*, vol. 14, no. 10, 2018.

[44] 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, pp. 32-45, Feb. 2016.

[45] P. Tyagi and D. Dembla, "Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)," *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 133-139, 2017.

[46] C. L. Chen, Y. X. Chen, C. F. Lee, Y. Y. Deng, and C. H. Chen, "An efficient and secure key agreement protocol for sharing emergency events in VANET systems," *IEEE Access*, vol. 7, pp. 148472-148484, 2019.

[47] A. Kchaou, R. Abassi, and S. G. E. Fatmi, "A new trust based routing protocol for VANETs," in *Proc. Seventh International Conference on Communications and Networking (ComNet)*, Nov. 2018, pp. 1-6.

[48] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "Trouve: A trusted routing protocol for urban vehicular environments," in *Proc. Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015, pp. 260–267.

[49] A. Tolba, "Trust-Based distributed authentication method for collision attack avoidance in VANETs," *IEEE Access*, vol. 6, pp. 62747-62755, 2018.

[50] 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, pp. 32 – 45, Jan. 2015.

[51] M. Wooldridge, N. R. Jennings, and D. Kinny, "The Gaia methodology for agent-oriented analysis and design," *Autonomous Agents and MultiAgent Systems*, vol. 3, no. 3, pp. 285–312, Sep. 2000.

[52] T. Xie and X. Qin, "Scheduling security-critical real-time applications on clusters," *IEEE Trans. Comput.*, vol. 55, no. 7, pp. 864–879, Jul. 2006.

[53] C. Douligeris and D. N. Serpanos, *Network Security: Current Status and Future Directions*, 1st ed. IEEE Press, 2007.

[54] M. Saleh and L. Dong, "Real-Time scheduling with security enhancement for packet switched networks," *IEEE Transactions on Network and Service Management*, vol. 10, no. 3, pp. 271-285, September 2013.

[55] Standard for local and metropolitan area networks - virtual bridged local area networks - amendment 5: Connectivity fault management (amendment to IEEE Std 802.1Q-2005, as amended by IEEE Std 802.1ad-2005)," IEEE Approved Draft Std P802.1ag/D8.1, Jun. 2007.

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.