Security Aware Routing Protocol for Intelligent Transportation Distributed Multi-Agent System

Ma'en Saleh
CCE Department
Tafila Technical University
Tafila, Jordan

ABSTRACT

Most recent VANETs routing protocols have neither taken into consideration security aspects nor the available resources at the mobile node. In this research, a security-aware road-side routing protocol with resource estimation methodology (SRSR_RE) for VANETs in a segmented road topology was proposed. The proposed algorithm was modelled by a distributed multi-agent system and to be installed at each road-side base-unit (RSU). The algorithm combines a congestion control unit that adopts a resource estimation mechanism with a secure-route discovery scheme. By such combination, both security and quality-of-service (QoS) requirements are guaranteed, and thus making our VANET robust against security threats besides protecting it from being congested. Compared to the insecure road-side (IRSR) and secure road-side (SRSR) protocols, extensive simulation results show the highest capability of the proposed protocol (SRSR_RE) in maximizing the secure delivery of the data packets and minimizing the end-to-end delays for VANETs with different network's factors such as nodes density, number of malicious nodes and node's buffer size.

Keywords

Keywords Routing, Security, Agents, Distributed Systems, VANETs, QoS, Resource Estimation, ITS, Road Segmentation, Security Threats.

1. INTRODUCTION

Intelligent transportation system (ITS) is a set of advanced electronics, technology, and telecommunication protocols that are applied to provide different layers of services that are related to traffic management and transportation [1]. Such services could be classified into two main categories: commercial-related and safety-related services [2]. Commercial-related applications provide convenience and comfort for its customers, such as map-download, internet transactions, electronic toll collection, and navigation [3]. From the other side, safety-related applications are designed to provide its customers with real-time life-critical information, such as collision warnings, emergency vehicle notifications, automatic road enforcement, and slow-down warnings [4-5].

Because of its promising and efficient solution to ITS, vehicular ad-hoc networks (VANETs) become a hot topic of research, where a number of vehicles act as mobile nodes in a mobile ad-hoc network (MANET) [6]. In order to provide an efficient communication between MANET nodes, different routing protocols were proposed, such as proactive (i.e., OLSR and DSDV), reactive (i.e., AODV and DSR), hybrid (i.e., ZRP), hierarchal (i.e., CBRR and FSR), fault-tolerant routing protocols (i.e., FTAR, LAFTRA, and WEFTR), and energy-based routing protocols (i.e., REEP, LEO, EAAR, BFIRIP) [7-16]. Although VANET is considered as a sub-class of MANET, different key factors make the routing protocols designed for MANETs not that efficient for VANETs. Such factors include: the high-speed mobility of the vehicles, highly-dynamic path topology, intermittent relative distance between vehicles, and signal-blocking objects [17-18]. Accordingly, different routing protocols for VANETs were designed to overcome the limitations of the MANET protocols, such as position-based routing protocols (i.e., GPSR, GPCR, and DD-LAR), cluster-based routing protocols (i.e., COIN, LORA-CBF, and CLARA), broadcast-based routing protocols (i.e., BROADCOMM and UMB), Geocast-based Routing (i.e., ZOR) [19-24].

Nowadays, providing a secure data communication for VANETs becomes a demand, where the data passed from one vehicle to another may be hacked by a malicious vehicle, and thus affects the safety-related services provided, which may lead to a catastrophe [25]. Several types of security threats could be defined for VANETs, such as ID altering, spoofing, GPS information hacking, and position cheating [26-27]. Accordingly, the VANETs routing protocols should be modified to be security-aware. To achieve that, different security-aware routing protocols were proposed, such as ARIADNE, CONFIDANT, SEAD, SAODV, SLSP, SLOSR, DLSR, Trust-Based Multi-Path Routing [28-34]. The previous routing protocols select a secure-route between the source and destination in a VANET network, and thus making the VANET robust against different layers of security threats.

Although the previous routing protocols are security-aware, the VANET may still suffering from losing information messages. Such loosing is not related to a malicious node, but to limited available resources (i.e., available buffer) at the intermediate nodes in the VANET. Such limitation may lead to congest the VANET, and thus degrade the quality-of-service level provided by the VANET. In the case of safety-related applications, such case may expose the driver's life to danger, where real-time messages should be available with a strict deadline. Accordingly, a security-aware routing protocol for VANETs was proposed to overcome such problem by deploying a resource estimation methodology for the resources of intermediate vehicles. Such resource estimation scheme will be integrated with the security-aware routing unit, and thus the route to be discovered is the most secure route with available resources. By implementing such design, both security and QoS requirements will be guaranteed [35], and thus protecting the network from both security threats and congestion.

Conventional simulation techniques are suitable for best-effort networks where no QoS or security guarantees are provided for the data traffics [36]. However, they are inefficient in modelling and analyzing complicated heterogeneous environments such as our highly-dynamic topology real-time VANET network with QoS guarantees and security aspects.

To overcome such inefficiency, the proposed algorithm was modelled using distributed agent-based methodology [37], where the road was virtually segmented. Each road-segment was modelled by a multi-agent system, where a set of sub-agents are cooperating to serve the real-time request generated by the source node. Collaboration between different multi-agent (different road-segments) where established to guarantee a continuous path of communication between two vehicles from different segments. The key features of the proposed security-aware routing algorithm are as follows:

1) Integrating the security-awareness unit with routing-discovery scheme, which makes the VANET robust against security threats, especially for those safety-related issues.
2) Deploying a resource estimation methodology for congestion control, and thus guaranteeing the QoS requirements of the system.
3) Designing the system using distributive agent-based methodology, and thus reducing the complexity of providing a reliable communication between the VANET nodes.

2. MULTI-AGENT DESIGN MODEL

To provide an efficient and reliable path of communication between the source and destination nodes, the proposed system was designed using a distributed agent-based system. According to the agent-based methodology, the road path was decomposed into virtual segments, where each segment is served by a road-side base unit (RSU) as shown in Fig.1.

The first phase of deploying the agent-based technology was the decomposition, where the entire multi-agent system at each road-segment was decomposed into six interactive sub-agents that belong into two main categories: (1) Hardware agents including source and intermediate nodes sub-agents; (2) Software agents including: route estimator, security model, resource estimator, and coordinator. Such software sub-agents were installed at the road-side unit (RSU). The main behaviors and functionalities of each sub-agent was defined in the modelling phase. Finally, protocol designing phase was performed to define the layer of communication and interaction between the sub-agents.

2.1 Source Agent

This is a hardware agent that represents a vehicle with a specific identification number and requests for secure route to send its traffic to the destination. The generated traffic by such agent will have a rate (λ), and thus an exponential distribution with a mean ($1/\lambda$) was used to generate the inter-arrival time for the traffic segments (Data packets).

2.2 Intermediate Node Agent

This hardware agent models the intermediate vehicles that used as a route between the source and destination. Each node has an identification number that is the plate number, which can be modeled as the MAC address in the communication protocol. The intermediate node has a well-defined memory resources, that is its available memory buffer (M).

2.3 Controller Agent

This software agent is to be installed at the road-side unit. It represents the core of our system that collects other agent's system information, evaluates system parameters, governs system functionalities, defines directions of data flows, adjusts system parameters to ensure proper services.

2.4 Route Estimator Agent

Such software agent is the one that is responsible of generating the routing table needed by each node to send its data traffic to anywhere in the network. It interacts with the security model sub-agent to provide a secure routing table that protects the entire system from being hacked by security threats.

2.5 Security Model Agent

In this software agent, the generated routing table by the route estimator will be examined for malicious nodes. This agent requires to interact with controller sub-agent for checking network acknowledgements to discover those malicious nodes as discussed in [38]. From the other side, it interacts with the resource estimator to find out the main reason of dropping data packets, that is due to threats or lack of resources.

2.6 Resource Estimator Agent

This agent is a software agent installed at the road-side. It called a tracker, where it tracks the memory resources of the intermediate nodes. It's the one that the security model depends on it to justify whether the node is a malicious node or not. This sub-agent could be used to provide a feed-back about the network's status to protect it from being congested by heavy traffic loads.

To guarantee both security and QoS requirements of the system, the proposed algorithm integrates two main units: secure-route discovery and congestion control units. Such units are the core of the controller's sub-agent design. The secure-route discovery unit is to be modelled by a secure routing protocol that selects the most secure route among a set of discovered routes between the source and destination nodes. The protocol uses a confidence level for the selection process. To protect the secure data from being sniffed while the coordinator identifies the secure route, we assume that the proposed protocol scheme works at the initiating process, where the source begins with fake data to discover the malicious node. From the other side, the congestion control unit adopts a resource estimation mechanism that ensures the capability of the secured route to serve the source request within QoS constraints.

According to the locations of the source and destination nodes, our algorithm was designed to operate in one of two modes: single-segment mode and multi-segment mode. In single-segment mode, both source and destination belong to the same virtual road-segment. Accordingly, single coordinator is controlling the secure-route selection process. From the other hand, multiple-segment mode will be activated when the source and destination don't belong to the same segment. In such case, a layer of cooperation between multiple RSUs exists to provide a continuous path of communication between the source and destination. In this mode, the controller for each segment should be able to identify the gate-way node, which is the node that connects two virtual segments via multiple-segment inter-vehicle communication.

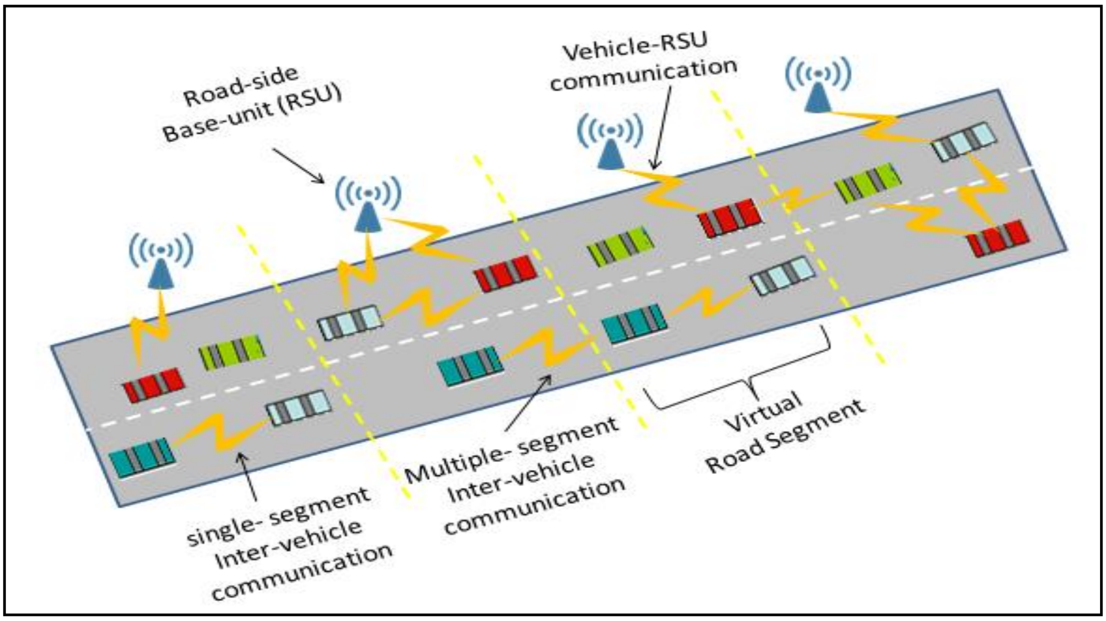

Fig 1: Road-Path Virtual Segmentation for Intelligent Transportation System (ITS)

3. SYSTEM PARAMETERS

To model our proposed secure routing protocol, different network parameters should be well defined such as the nodes mobility model, road-side and nodes parameters, threat model, security model, routing protocol, and communication scheme.

3.1 Assumptions

In this research, we assume a mobility model where nodes are moving in the same direction with a constant speed. Accordingly, within a time frame the positions of the nodes is fixed, implying route are also fixed. Each segment is covered by a road-side unit (RSU) that monitors all the vehicles in the segment (coverage the whole segment). The road side unit has a communication with the adjacent road-side units. We also assume that each node will be in the center of its transmission circle.

3.1.1 Road Segments

we assume that we have *X* number of road-segments with each segment has the following attributes:

1) The ID of the segment (S_{ID}).

2) The segment dimensions (*L, W*): *L* is the length of the segment, while *W* is the segment's width.

3.1.2 Mobile Nodes

We assume that there is *N* number of mobile nodes (vehicles) in each road segment with each node has the following attributes:

1) The node address (N_{ID}): Each vehicle node in the segment has a unique address that is the plate number (looks like the MAC address).
2) The road segment where the node belongs (*R*).
3) Available Memory Buffer for the node (*M*).
4) The security confidence level (*S*) that is between 0 and 1. Where 1 is the highest security confidence level, which means that the node is 100% trusted.
5) The node speed ($\hat{S}$): Nodes are moving in the same direction with a constant speed. (i.e. within a time frame the positions of the nodes is fixed, implying route are also fixed).
6) The node position (P_x, P_y).
7) The number of received packets by the node (P_r).
8) The number of packets forwarded by the node and received acknowledges from the next hop in the route (P_f).
9) Strength of signals received by the node from the road sides. We will assume that no more two signals could be received (α_1, α_2). Such parameters are the key behind defining the segments' boundaries.

3.2 Communication Schemes

Two main communication schemes are defined in our model as the following:

1) Intra-segment communication scheme: That is when the source and destination belong to the same segment. In such case, the coordination will be performed by single RSU.
2) Inter-segment communication: In such case, the source and destination belong to different segments. In such scenario, the communication between the source and destination will be operated through the cooperation between the adjacent RSUs.

3.3 Threat Model

Our model protects the VANET from two main security threats:

1) Man-in-the-middle attack (MITMA): It's a cyberattack that is well known in wireless communications, where a malicious node intercepts the communication between two parties through establishing independent connections with them that allow it to alter transferred data, send fake messages to them, and make them believe that they are directly connected over a private session [39].
2) Eavesdropping (Sniffer): Such attack is a network-layer hacking threat, where a malicious node starts listening to a channel between two parties and capturing the transferred data between them. Accordingly, the hacking node will be able to collect a metadata that provides it with the required

privileges needed to hack a whole secure system. The main thing that allows the sniffing process is that the transferred data lack of encryption. Our threat detection model is based on the secure route selection scheme that we propose in [38]. The proposed algorithm integrates a resource estimation method with a security-based unit (SRREM) using agent-based technology for secure route selection. Once the secure route was selected by SRREM, the union protocol was used to guarantee such secure route. In union protocol, the RSU will use a public key encryption scheme. Accordingly, any other node not in the route and receives the data will not be able to take any further action other than dropping the data packet.

4. SYSTEM METHODOLOGY

Our system methodology depends on five main phases performed by the cooperated agents in the multi-agent design model. Such phases include: route discovery, building routing table, resource estimation, secure selection, and building secure route table as shown in Fig. 2.

To understand the communication scheme between the sub-agents in our proposed agent-based system, an example that describes the whole interaction process along with the sub-agent functionalities is provided. Fig.3 shows a scenario of two virtual road-segments, where each segment is controlled by a single road-side unit RSU (RSU_1 and RSU_2) to coordinate the communication between N vehicles in a VANET network. (i.e. N is set to nine vehicles).

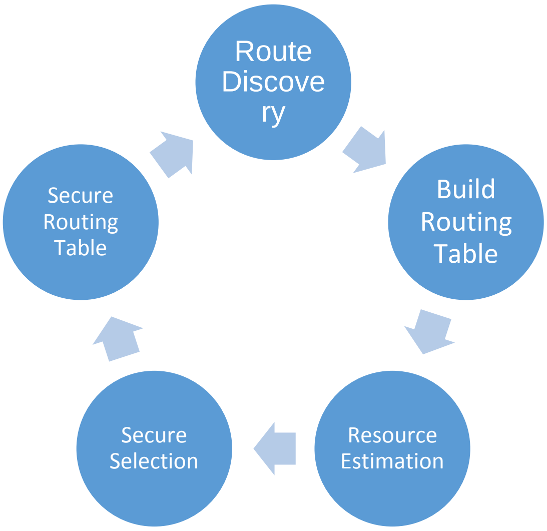

Fig 2: Agent-Based System Phases

The process begins when a source agent requesting for a secure route by sending a control message to the controller. Accordingly, the controller broadcasts a control message in the segment requesting the nodes to send their adjacent lists. Upon receiving such broadcasted control signal, each node starts to build a list of adjacent nodes (A). (i.e. Table 1 shows the adjacent lists for the communicated nodes in segment 1 shown in Fig.3).

Table 1. Adjacent List

Node	Adjacent List (A)
1	$A_1 = \{2\}$
2	$A_2 = \{1, 3, 5\}$
3	$A_3 = \{2, 4, 5\}$
4	$A_4 = \{3, RSU_1\}$
5	$A_5 = \{2, 3, 6\}$
6	$A_6 = \{5, 7\}$
7	$A_7 = \{6, 8\}$

Here, a vehicle node may receive request signals from two road sides, especially those intermediate nodes such (i.e. node 7 and node 8). In this case, the node will respond to the strongest signal. Accordingly, a signal strength comparator is existing in each node. It also sends a packet indicating that it's an intermediate. The RSU keep tracks of those intermediate nodes in a list called I. (i.e. $I_1 = \{7\}$, $I_2 = \{8\}$). In order to avoid both hidden station problem (multiple nodes being able to see the road-side unit, but not each other) and collisions in such wireless network, carrier sense multiple access with collision avoidance (CSMA/CA) protocol was deployed at the data-link layer of the OSI model.

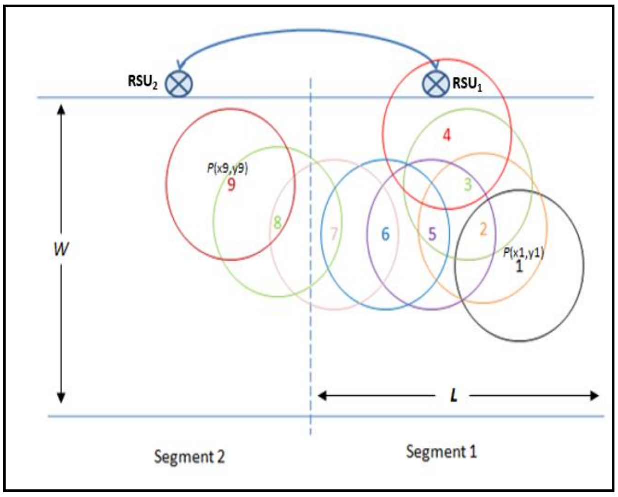

Fig 3: Road Segmentation

Once the adjacent list is defined by each node, the node responds to the previous request from the RSU by broadcasting its adjacent list (destination address is RSU). The adjacent nodes receive such transmissions and broadcasts it until arrive the destination (RSU). (i.e. In Fig.3, once node 1 identifies the list (A_1), it broadcasts it. The request arrives to node 2. Since node 2 is not the destination (RSU_1), it broadcasts it to nodes 1, 3, and 5. The process continues till a broadcast from node 4 arrives to RSU_1 (specifically, to the controller agent inside the RSU).

Once the controller receives the lists, it sends them to the route estimator sub-agent. Accordingly, the route estimator generates a routing tree for the segment, that is the initial unsecure routing table needed by the nodes to reach their destinations. It sends such routing tree to the controller. (i.e. Fig. 4 shows the generated routing tree for segment 1).

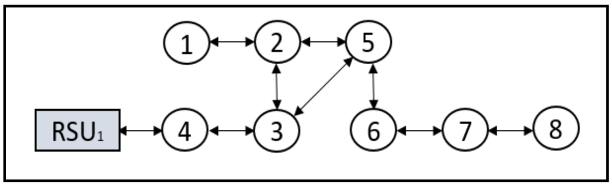

Fig 4: Initial Routing Tree

Our proposed algorithm adopts the secure route selection scheme that we propose in [38]. The proposed algorithm integrates a resource estimation method with a security-based unit (SRREM) using agent-based technology for secure route selection. Such algorithm depends on the intermediate nodes' acknowledgements on the transmitted fake data by the controller at the initiating process. The controller begins with such fake data to protect the secure data from being sniffed while identifying the secure route. Upon receiving such acknowledgements, the controller passes them to the security model sub-agent. The security model cooperates with the resource estimator sub-agent to discover the malicious nodes based on the SRREM. It distinguishes between four security cases: (1) case A: secure route; (2) case B: malicious node; (3) case C: Use resource estimation methodology; and (4) case D: use other routes to judge as discussed in [38].

According to case C, the security model sub-agent sends the node status to the resource estimator sub-agent to check whether the dropping of the packets was due to a malicious node or due to the lack of resources. Accordingly, the resource estimator requests for the resources of the node from the controller. The controller then passes such resource information to the estimator that performs the estimation process and sends the status back to the security model sub-agent. The security model sub-agent then sends the list of malicious nodes to the route estimator sub-agent, that in turns modifies the routing tree by dropping all malicious nodes from it. It then sends the updated secure routing tree to the controller. Upon receiving such tree, the controller responds to the source with the required secure route to the destination. Note that, secure route selection results in several routes that are categorized as classes based on some metrics (i.e., number of hops in the route).

According to the communication schemes categorized before we provide the following two scenarios (i.e. assuming that the routing tree in Fig.4 is the secure one):

1) Intra-segment communication scheme: That is when the source and destination belong to the same segment. i.e. If node 1 requests the controller at RSU_1 for a secure route to node 3. The controller checks the secure routing tree and finds that the best secure route is {1 → 2 → 3} and send it back to node 1. The controller applies then the onion protocol (public key encryption scheme). Accordingly, any other node not in the route and receives the data will not be able to take any further action other than dropping the data packet {i.e. Node 5}.
2) Inter-segment communication: In such case, the source and destination belong to different segments. i.e. If node 1 requests the controller at RSU_1 for a secure route to node 9. The controller checks the secure routing tree and finds that node 9 is not in its segment. Accordingly, the controller at RSU_1 communicates with the controller at RSU_2 asking for a route to node 9 through an intermediate node. The controller at RSU_2 finds the route {8 → 9} where (node 8 $\in I_2$) and sends the route to the controller at RSU_1. Accordingly, RSU_1 controller checks and finds that (node 8 $\in A_7$) and thus finds a route through node 7, that is: {1 → 2 →5 → 7} and sends it back to node 1. Then the onion protocol is added again to guarantee the delivery through such secure route. The interaction scheme for the multi-agent system is described in Fig. 5.

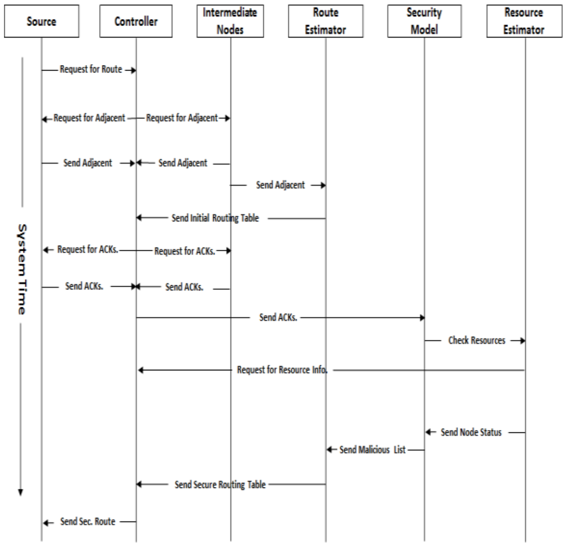

Fig 5: Agent-Based Communication Protocol

5. SIMULATION RESULTS

The conventional network simulators are not sufficient for analyzing complicated heterogeneous environments such as the dynamic real-time VANET with QoS guarantees and security aspects. From the other hand, simulators like NS2 are suitable for those wireless and mobile-ad hoc network, but geographical routing is not available in its standard code. Since our model is a multi-agent based scheme with its core sub-agents are software based agents, the simulation model was implemented based on the .Net platform, where the model is an object-oriented that provides a mechanism to inherit the methodologies used to design the interactions between the agents. It also allows the agents to synchronize with time-critical events.

A real-time VANET was simulated for different values of nodes (vehicles), that is N = {10, 20, 30, ----, 100}. We assume that we have two road-segments with each segment with the dimensions (L, W) were set to (500 m, 60 m). We assume that the number of nodes in each segment equals to N/2 nodes. In each simulation step, we assume that we have (N/2) peer to peer communications (source, destination) as the following: (n_i, $n_{i+(N/2)}$), where ni is the i^{th} node and i = {1, 2, -----, N/2}. The node's position (P_x, P_y) will be set randomly to be within the segment: $P_x \in (0, 500)$ and $P_y \in (0, 60)$. The sending rate in the initiating process (λ_i) is 40 packets/s, while the sending rate in the data communication phase (λ_d) is 200 packets/s with each node sends for 5 seconds (a total of 1000 packets) to the destination. Initially, the nodes will be given the highest security confidence level (S = 1) till modified by the RSU.

To show the performance of the proposed security-aware road-side routing protocol with resource estimation methodology (SRSR_RE), it was compared with two other implemented protocols: (1) Insecure road-side routing protocol (IRSR): In such case, each source will send the packets following the discovered non secure routing protocol by the route estimator (no security model either resource estimator sub-agents); (2) Secure road-side routing protocol (SRSR): In such protocol, an initial sending phase will occur to discover the malicious nodes. Here, the only trusted node is the road-side (RSU). Accordingly, the new peer communications will be (RSU, $n_{i+(N/2)}$), where *n*i is the i^{th} node and *i* = {1, 2, ------, *N*/2}. Once a malicious node is discovered, it will be dropped from the routing table and all the routes containing such node (no resource estimator sub-agent). The performance metrics to be measured are in terms of secure data delivery and average end-to-end delay taking into considerations different network's factors such as nodes density, number of malicious nodes and node's buffer size.

5.1 Effect of Vehicles Density

In this simulation, we demonstrate the performance of the proposed scheme in terms of both percentage of average secured data delivered from the source to the destination and the average total packets delay. The simulations were performed over a real-time VANET for different node densities (*N* = {10, 20, 30, ----, 100}). In such simulations, the percentage of malicious nodes (MITMA) was set to be 10%, while the buffer size was set to be a ratio of the sending rate ($M = \lambda_d/2$). Fig. 6 shows the performance of our proposed scheme (SRSR_RE) over the other routing protocols (IRSR and SRSR) in terms of secure delivery for the data packets. Such result is expected, where the IRSR doesn't take into consideration any malicious node in the route, then the network is opposed to be hacked by security threats. From the other side, SRSR may consider a node to be malicious and drop it from the routing table while it's not a malicious node. Such dropped node may be a secure node that lack of resources, so that it drops the packets. Since SRSR doesn't implement a resource estimator, it considers such node as a malicious node and skip it from the routing table. Such skipping may eliminate a unique secure route from the source to the destination and thus decreases the percentage of secure delivery.

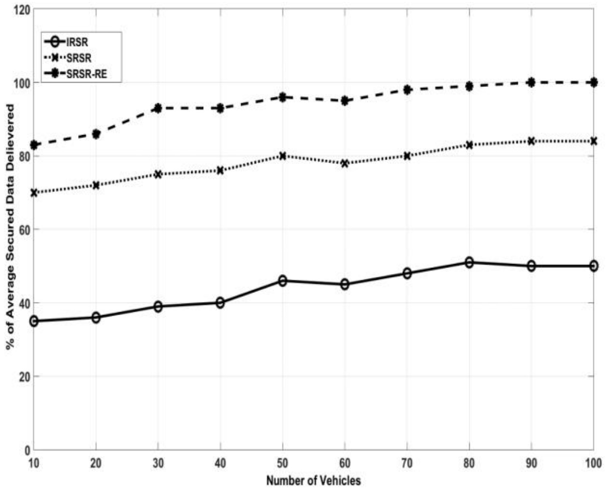

Fig 6: Effect of Node Density on Delivery

The other metric to be studied in this simulation is the effect of node density with a fixed percentage of malicious nodes on the average total packets delay. Fig.7 shows that IRSR has the lowest delay followed by SRSR_RE, while SRSR has the highest delay. This result doesn't reflect the performance of IRSR over the secure protocols, where the results has been taken based on the delivered packets not the total transmitted packets. The IRSR doesn't follow any security considerations, and thus it chooses the route with a minimum number of hops regardless the security status of the nodes. As a result, the packets end-to-end delay will be lower for such protocol. Accordingly, when security is taken into consideration, our proposed scheme shows higher efficiency over the SRSR in minimizing the end-to-end delay for the packets. Such result is due again to the dropping mechanism by the SRSR for a secure node that lacks resources. Such dropping may lead into considering a secure route with more number of hops to the destination, while it could be done through such dropped secure node that minimizing the number of hops in the route.

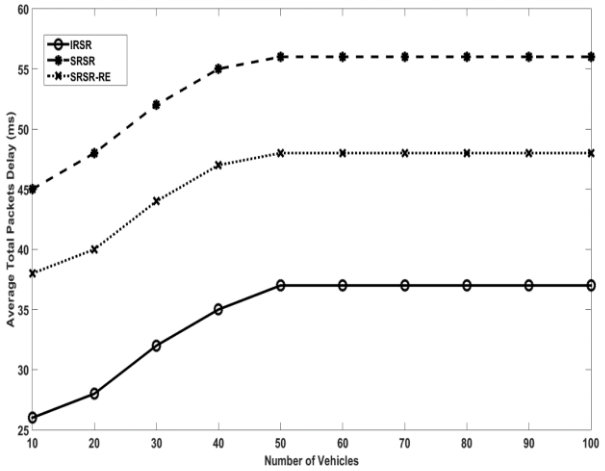

Fig 7: Effect of Node Density on Delay

5.2 Effect of Security Threats

In this simulation, we show the effect of the threat model on the performance of the three routing protocols (IRSR, SRSR, and SRSR_RE). The metrics to be studied here are both secure delivery and total average packets delay. To perform that, a real-time VANET was simulated with a node density (*N* = 60) nodes and a buffer ($M = \lambda_d/2$). The simulation was performed for different values of malicious nodes (Malicious Nodes = {3, 6, 9, 12, 15, 18}). Fig.8 shows that as the number of malicious nodes increases, the percentage of secure data delivery for the three protocols decreases. From the other side, the simulation result shows the capability of the proposed scheme (SRSR_RE) of delivering the data packets with a percentage up to (91%) in such type of environments, where a high percentage of threats (30%) is coexists.

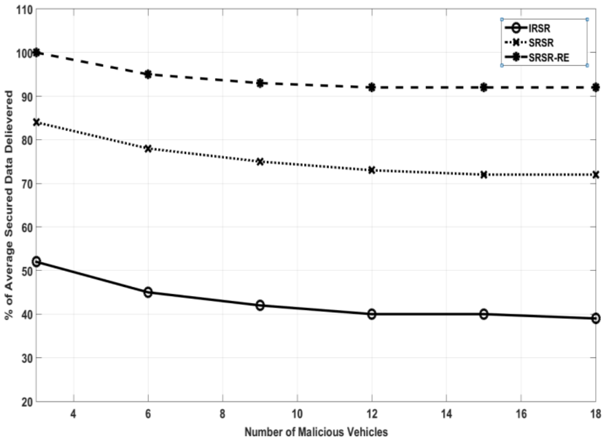

Fig 8: Effect of Malicious Nodes on Delivery

The effect of the malicious nodes on the total packets delay is shown in Fig.9. The simulation result shows that more malicious nodes yield into higher end-to-end delays. Compared with SRSR protocol, simulation results show the ability of SRSR_RE in minimizing the end-to-end delays with a percentage up to (9%) for a threat case of (30%). As we can see from the figure, the delays for the IRSR doesn't affected by increasing the number of malicious nodes, where such delays are calculated for those arrived packets not the total number of transmitted packets. The packets in IRSR will have the minimum trip time, where the route has the minimum number of hops, regardless the security status of the nodes.

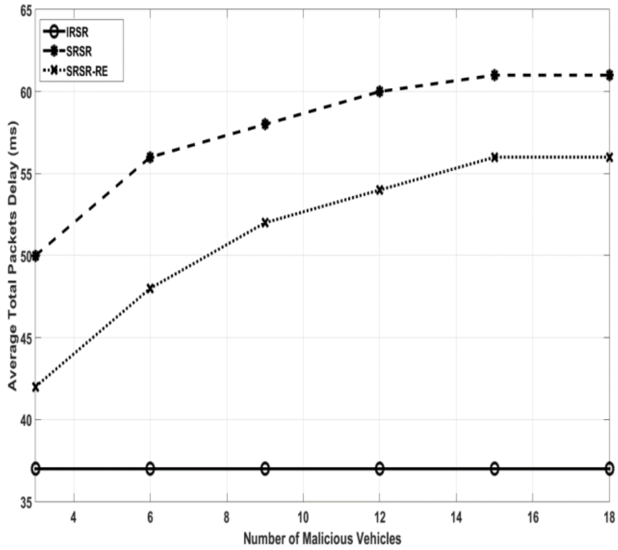

Fig 9: Effect of Malicious Nodes on Delay

5.3 Effect of Initial Buffer Size

In this simulation, we show the effect of the node's resources (initial buffer size *M*) on the percentage of secure data delivery and the average total packets delays for the three routing protocols (IRSR, SRSR, and SRSR_RE). In order to perform that, we simulate a real-time VANET with a node density (N = 60) nodes and a percentage of malicious nodes (MITMA) to be 10%. The simulation was performed for different values initial buffer size (M= {0.1, 0.3, 0.5, 0.7, 0.9, 1} * λ_d). Simulation results shows that the secure delivery of the packets increases as the initial buffer increases as shown in Fig.10. It also shows that our proposed scheme (SRSR_RE) provides the highest delivery of the packets compared with the other two protocols (IRSR and SRSR). The simulation results also show that both SRSR and SRSR_RE have the same performance for the unbounded buffer ($M = \lambda_d$), where the SRSR will not consider a node to be a malicious node, while it's not and lacks resources.

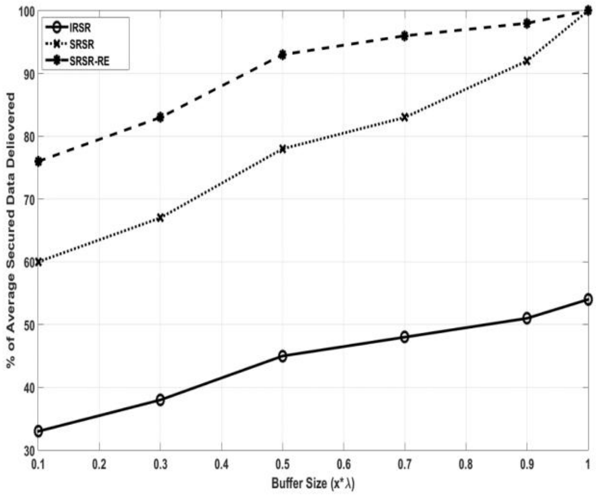

Fig 10: Effect of Buffer Size on Delivery

The effect of the initial buffer size on the total packets delay is shown in Fig.11. The simulation result shows that as the buffer size increases, the average delays decrease. Such result is expected, where the number of dropping nodes is decreases and thus they will be included in the secure routes, which may lead in routes with minimum number of hops. As a result, the total packets delay will be decreases as the packets trip is minimized. The result also shows that SRSR_RE outperforms the RSRS with a percentage up to (15%). Again, the ISRS will not be affected for the same reasons discussed before in section 5.2.

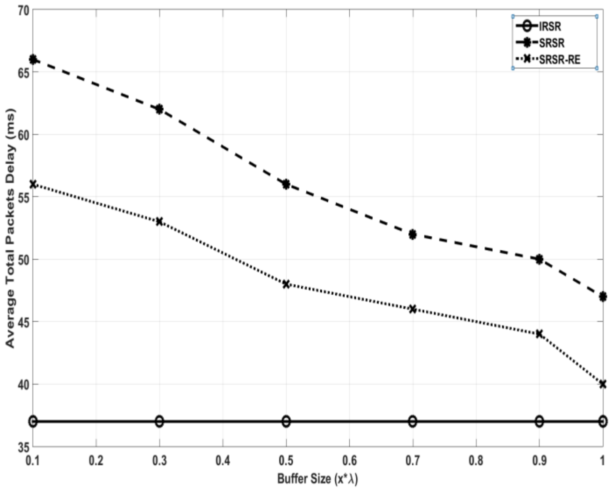

Fig 11: Effect of Buffer Size on Delay

6. CONCLUSION

In this research, a distributed multi-agent system was proposed to model a cooperation layer between a security-aware road-side routing protocol and a resource estimation methodology (SRSR_RE) for VANETs in a segmented road topology. Such combination is the key behind providing both QoS and security aspects for the VANET, where hacking and altering the transmitted information through the VANET may cause a catastrophe, especially that life-critical information such as driver ID, the location of the vehicle, or any other private data shared among a secure VANET. The proposed protocol outperforms the SRSR and the IRSR protocols in terms of the percentage of secure data delivery for networks with different factors such as nodes density, number of malicious nodes and node's buffer size. From the other side, the SRSR-RE outperforms the SRSR in the average total packets delay. Such metric is the key behind guaranteeing the QoS requirements for the real-time data flows.

7. REFERENCES

[1] Z. C. Taysi and A.G. Yavuz, "Routing Protocols for GeoNet: A Survey," IEEE Transactions on Intelligent Transportation Systems, vol.13, no.2, pp.939-954, Jun. 2012.

[2] A. Bouhoute, I. Berrada, and M. El Kamili, "A formal model of human driving behavior in vehicular networks," International Conference on Wireless Communications and Mobile Computing (IWCMC), pp. 231-236, Aug. 2014.

[3] M. J., Cobo, F. Chiclana, A. Collop, J. de Ona, and E. Herrera-Viedma, "A Bibliometric Analysis of the Intelligent Transportation Systems Research Based on Science Mapping," IEEE Transactions on Intelligent Transportation Systems, vol. 15, no. 2, pp. 901-908, Apr. 2014.

[4] N. Sánchez, J. Alfonso, J. Torres, and J . M. and Menéndez, "ITS-based cooperative services development framework for improving safety of vulnerable road users," Intelligent Transport Systems, IET, vol. 7, no. 2, pp. 236-243, Jun. 2013.

[5] C. Yung-Cheng and H. Nen-Fu, "An Efficient Traffic Information Forwarding Solution for Vehicle Safety Communications on Highways," IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 2, pp. 631-643, Jun. 2012.

[6] M. Sood and S. Kanwar, "Clustering in MANET and VANET: A survey," International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), pp. 375-380, Apr. 2014.

[7] H. Xu, X. Wu, H. R. Sadjadpour, and J. J. Garcia-Luna-Aceves, "A unified analysis of routing protocols in MANETs," IEEE Transactions on Communications, vol. 58, no. 3, pp. 911-922, Mar. 2010.

[8] T. P. Venkatesan, P. Rajakumar, and A. Pitchaikkannu, "Overview of Proactive Routing Protocols in MANET," Fourth International Conference on Communication Systems and Network Technologies (CSNT), pp. 173-177, Apr. 2014.

[9] M. K. Gulati and K. Kumar, "A review of QoS routing protocols in MANETs," International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6, Jan. 2013.

[10] S. Misra, S. K. Dhurandher, M. S. Obaidat, K. Verma and P. Gupta, "A Low Overhead Fault-Tolerant Routing Algorithm for Mobile Ad-Hoc Networks Based on Ant Swarm Intelligence", Simulation Modelling Practice and Theory (Elsevier), vol. 18, no. 5, pp. 637-649, 2010.

[11] S. Misra, P. V. Krishna, A. Bhiwal, A. S. Chawla, B. E. Wolfinger, C. Lee, "A Learning Automata-Based Fault-Tolerant Routing Algorithm for Mobile Ad Hoc Networks", The Journal of Supercomputing (Springer), vol. 62, no. 1, pp. 4-23, Oct. 2012.

[12] B. J. Oommen and S. Misra, "Fault-Tolerant Routing in Adversarial Mobile Ad Hoc Networks: An Efficient Route Estimation Scheme for Non-Stationary Environments", Telecommunication Systems (Springer), vol. 44, nos. 1-2, pp. 159-169, Jun. 2010.

[13] S. Misra and D. Thomasinous, "A Simple, Least-Time, Energy-Efficient Routing Protocol with One-Level Data Aggregation for Wireless Sensor Networks", Journal of Systems and Software (Elsevier), vol. 83, no. 5, pp. 852-860, May 2010.

[14] F. Zabin, S. Misra, I. Woungang, H. Rashvand, N.-W. Ma and M. A. Ali, "REEP: A Data-Centric, Energy-Efficient and Reliable Routing Protocol for Wireless Sensor Networks", IET Communications, vol. 2, no. 8, pp. 995-1008, 2008.

[15] S. Misra, S. K. Dhurandher, M. S. Obaidat, P. Gupta, K. Verma and P. Narula, "An Ant Swarm-Inspired Energy-Aware Routing Protocol for Wireless Ad-Hoc Networks", Journal of Systems and Software (Elsevier), vol. 83, pp. 2188-2199, 2010.

[16] S. Misra and G. Rajesh, "Bird Flight-Inspired Routing Protocol for Mobile Ad Hoc Networks", ACM Transactions on Autonomous and Adaptive Systems, vol. 6, no. 4, Article 25, Oct. 2011.

[17] M. T. Barros, R. C. Gomes, and A. F. Costa, "A Top-down Multi-Layer Routing Architecture for Vehicular Ad-Hoc Networks," IEEE Latin America Transactions, vol. 11, no. 6, pp. 1344-1352, Dec. 2013.

[18] [18] F. Z. Bousbaa, N. Lagraa, and M. B. Yagoubi, "Novel geocast routing protocols for Safety and Comfort Applications in VANets," IEEE Globecom Workshops (GC Wkshps), pp.1308-1313, Dec. 2013.

[19] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," IEEE Vehicular Technology Magazine, vol. 2, no. 2, pp. 12-22, Jun. 2007.

[20] H. Saleet, R. Langar, K. Naik, R. Boutaba, A. Nayak, and N. Goel, "Intersection-Based Geographical Routing Protocol for VANETs: A Proposal and Analysis," IEEE Transactions on Vehicular Technology, vol. 60, no. 9, pp. 4560-4574, Nov. 2011.

[21] S. Allal and S. Boudjit, "Geocast Routing Protocols for VANETs: Survey and Guidelines," Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 323-328, Jul. 2012.

[22] C. Barba, L. Aguiar, and M. Aguilar, "Design and evaluation of GBSR-B, an improvement of GPSR for VANETs," IEEE Latin America Transactions, vol. 11, no. 4, pp. 1083-1089, Jun. 2013.

[23] N. Kumar, S. Misra and M. S. Obaidat, "Collaborative Learning Automata-Based Routing for Rescue Operations in Dense Urban Regions Using Vehicular Sensor Networks," in IEEE Systems Journal, vol. 9, no. 3, pp. 1081-1090, Sept. 2015.

[24] K. Pandey, S.K., Raina, and R.S. Raw. "Distance and direction-based location aided multi-hop routing protocol for vehicular ad-hoc networks", Int. J. Communication Networks and Distributed Systems, vol. 16, no. 1, pp.71–98, 2016.

[25] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," IET Communications, vol. 4, no. 7, pp. 894-903, Apr. 2010.

[26] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in VANETs," Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp.1-6, Jul. 2013.

[27] 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.

[28] M. Rajeswari, P. U. Maheswari, S. Bhuvaneshwari, and S. Gowri, "Performance analysis of AODV, DSR, TORA and OLSR to achieve group communication in MANET," Fourth International Conference on Advanced Computing (ICoAC), pp.1-8, Dec. 2012.

[29] T. Bouali, E. Aglzim, and S. Senouci, "A secure intersection-based routing protocol for data collection in urban vehicular networks," IEEE Global Communications Conference (GLOBECOM), pp.82-87, Dec. 2014.

[30] M. Pura, B. Ion, and V. Patriciu, "On modeling and formally verifying secure explicit on-demand ad hoc routing protocols," International Conference on Software Technology and Engineering (ICSTE), vol. 2, pp. 215-220, Oct. 2010.

[31] W. Xi, S. Liu, H. Zhu, Y. Zhao, and C. Lei, "Modeling and Verifying the Ariadne Protocol Using CSP," IEEE International Conference and Workshops on Engineering of Computer Based Systems (ECBS), pp.24-32, Apr. 2012.

[32] J. Toutouh, J. Garcia-Nieto, and E. Alba, "Intelligent OLSR Routing Protocol Optimization for VANETs," IEEE Transactions on Vehicular Technology, vol. 61, no. 4, pp. 1884-1894, May 2012.

[33] S. Misra, P. V. Krishna, K. I. Abraham, N. Sasikumar and S. Fredun, “An Adaptive Learning Routing Protocol for the Prevention of Distributed Denial of Service Attacks in Wireless Mesh Networks”, Computers & Mathematics with Applications (Elsevier), vol. 60, no. 2, pp. 294-306, 2010.

[34] P. Narula, S. K. Dhurandher, S. Misra and I. Woungang, “Security in Mobile Ad-Hoc Networks Using Soft Encryption and Trust-Based Multi-Path Routing”, Computer Communications (Elsevier), vol. 31, no. 4, pp. 760-769, 2008.

[35] N. Al-Oudat and G. Manimaran. “Task scheduling in heterogeneous distributed systems with security and QoS requirements”, Int. J. Communication Networks and Distributed Systems, vol. 9, nos. 1/2, pp.21–36, 2012.

[36] S. L. Spitler and D. C. Lee, "Integration of Explicit Effective-Bandwidth-Based QoS Routing with Best-Effort Routing," IEEE/ACM Transactions on Networking, vol. 16, no. 4, pp. 957-969, Aug. 2008.

[37] 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, Sep. 2013.

[38] M. Saleh, A. Aljaafreh, and N. Al-Oudat, "Secure Route Selection Based on Resource Estimation Methodology using Agent-Based Systems for Limited Resources WSNs," 9th International Conference on Computer Engineering and Applications, pp. 423-428, Feb. 2015.

[39] M. Shah, V. Soni, H. Shah and M. Desai, "TCP/IP network protocols — Security threats, flaws and defense methods,"3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp. 2693-2699, Mar. 2016.