Secure Traffic Efficiency Control Protocol for Downtown Vehicular Networks

Maram Bani Younes
(Corresponding author: Maram Bani Younes)
Computer Science Department, Philadelphia University, Jordan
P. O. Box: 19392 V Amman - Jordan
(Email: mbani047@uottawa.ca)
(Received Nov. 6, 2017; Revised and Accepted June 18, 2018; First Online Feb. 26, 2019)

Abstract

The intelligent transport system increasingly considers the traffic efficiency applications over the road networks. This type of application aims mainly at reducing the traveling time of each vehicle toward its targeted destination/destinations and deceasing the fuel consumption and the gas emissions there. The Vehicular Ad-Hoc Networks (VANETs) technology is one of the main approaches that have been used in these applications. However, the connecting environment of VANETs introduces a good chance for malicious drivers to take advantages of other cooperative drivers and deceive them to achieve their own benefits. This paper introduces a Secure Traffic Efficiency control Protocol (STEP). The designed protocol means to secure the traffic efficiency control applications over the downtown areas. It protects the privacy of cooperative drivers and minimizes any damage that malicious drivers may cause. From the experimental results, the STEP protocol succeeds to detect malicious nodes over the road network. Thus, it enhances the correctness of the traffic efficiency applications and increases their feasibility.

Keywords: Authentication; Integrity; Malicious; STEP; Traffic Efficiency

1 Introduction

Several protocols have been introduced recently aiming to efficiently use the available resources over the downtown road scenarios [4,12,20,32]. The grid-layout of the modern downtown areas directs the researchers to develop protocols that first evaluate the real-time traffic characteristics of each road segment separately [34,39]. Then, according to the traffic distribution over the downtown area, several research studies have selected the best path toward any targeted destination in terms of traveling time [38], fuel consumption and gas emission [25, 40] or the context of each road segment [33]. Moreover, located traffic lights are significant in term of controlling the traffic efficiency. Several protocols have been introduced aiming to intelligently schedule the phases of each traffic light based on the traffic distribution over the neighboring road segments [23, 36, 37].

Several security issues are threaten the traffic efficiency protocols over the downtown areas [18]. Indeed, these issues have dangerous consequences when attackers exploit the venerabilities in the traffic efficiency protocols. Malicious attackers can be categorized into four main groups according to their targets: Vandal, selfish, intruder, and prankster. Vandal attackers aim to overload the network with useless packets, which causes losing important data and decreasing the functionality of the connecting network. Selfish attackers deceive other drivers, in order to achieve their own benefits while falsely direct the traffic. Intruders try to chase and stalk other drivers and their end destinations. finally, pranksters and criminals may try to deceive drivers in a certain area aiming to kidnap or hurt them.

In this work, we introduce a secure traffic efficiency control protocol (STEP) for downtowns, using the communication technology of VANETs. This protocol aims mainly to achieve the authenticity and the integrity of the transmitted data. Thus, it guarantees the correctness of the targeted efficiency control factor (*i.e.*, traveling time, traveling speed, fuel consumption, gas emission, *etc.*)

The remaining of this paper is organized as follows: In Section 2, we investigate some traffic efficiency control protocols and other traditional secure protocols that have been introduced using the communication technology of VANETs. We then define the general adversary threats of traffic efficiency protocols in Section 3. Next, the details of the secure traffic efficiency control protocol (STEP) is presented, in Section 4. After that, we present the experimental study which evaluates the efficiency, accuracy, and correctness of the STEP protocol compared to other unsecure traffic control protocols in Section 5. Eventually, Section 6 presents the entire conclusion of this work.

2 Related Work

In this section, we investigate the details of some traffic efficiency control protocols that have been developed using VANETs for downtown areas. After that, we explore some traditional secure protocols that have been designed for VANETs.

2.1 Traffic Efficiency Control Protocols

Several protocols have been introduced in the literature to control the traffic efficiency over the road network [11,13, 20,23,28,33,34,36,38]. These protocols aimed to enhance traffic fluency of vehicles on the road network. This is by decreasing the traveling time, the fuel consumption and the gas emission. It is also by increasing the traveling speed of each vehicle toward its destination.

The grid-layout of the downtown areas motivates the researchers in this field to investigate and locate the highly congested road segments. Then, recommend drivers to avoid these congested road segments during their trips. On the other hand, intelligent scheduling algorithms have been introduced for the installed traffic lights on downtown areas. These algorithms aim to decrease the waiting delay time of each vehicle at the signalized road intersections. Some of these algorithms use the traffic distribution on the neighboring road segments. Others consider the estimated arrival time of competing traffic flows.

2.1.1 Traffic Congestion Detection

The existed traffic evaluation and congestion detection protocols are classified into two main categories: Sensor-based protocols [7, 21, 27] and vehicular-based protocols [13,28,34,39].

The sensor based protocols provide real-time and accurate congestion level estimation for each investigated road segment. However, in these protocols special and expensive equipments (*e.g.*, camcorders, inductive loop detectors, antennas, radars, *etc.*) are required all over the area of interest. It is difficult to install and maintain these equipments regularly. Moreover, these equipments provide fixed-point or short-section traffic information limitations [21]. The basic traffic data is extracted from vehicles passing through the detection zone and saved for farther usage or analysis.

On the other hand, different traffic evaluation protocols have been introduced using the technology of VANETs. These protocols collect the basic traffic data of surrounding vehicles in each traveling zone. Traveling vehicles are expected to be equipped by VANETs-wireless transceiver and Global Positioning System (GPS) devices. Traveling vehicles broadcast their basic data periodically in order to announce their location, direction and speed during that period of time. Receiver vehicles can compute and/or predict the traffic density [13,39], traffic speed, or traveling time [42] of that area, using the gathered traffic data of the surrounding vehicles.

In order to expand the boundaries of the investigated area, Fukumoto *et al.* [13] used a blind forwarding mechanism where each vehicle forwards the received messages. On the other hand, Sankaranarayanan *et al.* [28] proposed a more efficient mechanism that forwards statistical data of the traffic situation over the area of interest. In our previously proposed work [34], we have introduced a protocol that specifically aimed to evaluate the traffic characteristics on any road segment in a downtown area. Based on the length of each road segment, reporting areas are virtually configured on that road where vehicles over these areas are responsible of forwarding the gathered traffic data. This mechanism aims mainly to deliver the traffic information between vehicles that cannot contact directly.

2.1.2 Road Traffic Control and Efficient Path Recommendations

Different protocols have been introduced to select the best path (*i.e.*, most efficient) toward each targeted destination. The grid-layout of the downtown area contains different paths that lead toward any targeted destination. Several protocols [4, 12, 20, 42] have used a central processor that gathers the real-time traffic distribution all over the investigated road network. The best or fastest path toward each targeted destination is obtained by the central processor. The best path recommendations are sent back to each traveling vehicle all over the area of interest. However, this centralized behavior introduces a bottleneck as well as single point of failure problems [30].

On the other hand, several researchers have designed a complete distributed path recommendation and congestion avoidance protocols [32, 33]. The best path toward each targeted destination is obtained and updated in a hop-by-hop fashion. The path is then constructed from the location of the targeted destination toward each road intersection all over the area of interest. Periodic and dynamic communications take its place among installed RSUs at each road intersection, in order to ensure full awareness of real-time traffic characteristics.

Furthermore, several protocols have been proposed to recommend the best path in terms of fuel consumption or gas emission [25, 40]. Other studies have considered the context of the road network [33] in terms of located services at each road segment. They aim to guarantee a certain level of congestion-free to special road segments (*e.g.*, a congestion-free level is guaranteed for road segments that lead to hospitals in order to allow the emergency cases to arrive it fast).

2.1.3 Intelligent Traffic Light Control

In order to design an intelligent scheduling algorithm for located traffic lights on downtown road networks, several mechanisms have been proposed. Some studies have introduced a scheduling algorithm for isolated traffic light (*i.e.*, single assumed traffic light) [15,16,24]. These studies have considered the real-time traffic characteristics of

competing flows of traffic at a single road intersection. Traffic volume and the length of vehicles' queues [31], traffic speed and density [36] and estimated arrival times [23] are the main real-time parameters that have been considered to obtain efficient schedules for isolated traffic lights.

Several other studies have considered the cooperative communications among located traffic lights over road networks [22, 37, 41]. These studies have produced scheduling algorithms for each traffic light located on close road network or open road networks. It is referred to the synchronized situation among located traffic lights on grid-layout road network where all road segments have the same priority to cross the signalized intersection as close road network [14]. On the other hand, the scenarios where an arterial street (*i.e.*, set of continues road segments) is existed on the road network vehicles over this street have a higher priority to cross any signalized intersection before conflicted traffic flows is referred to as open network [29].

For the open and close road network scenarios. Besides, considering the traffic characteristics of the competing traffic flows, the schedule of each traffic light in these scenarios have considered the estimated arrival platoons of vehicles from the neighboring road intersections [5,22,41]. The number of vehicles, traveling speed and estimated arrival time of each platoon are the main characteristics to consider in these algorithms.

2.2 Secure Protocols for VANETs

The high speed mobility and extended geographical area of the VANET technology have produced real challenges to secure the introduced applications there. Special mechanisms have been designed to enhance the secure communications on VANETs. Several studies have been introduced to guarantee the authenticity, integrity and confidentiality feature for VANET in general [9, 10, 17].

Recently, researchers start developing secure service protocols. These protocols provide a certain service and specifically considering the security requirements of that service. To mention a few, secure cooperative collision warnings [26], secure position information [3], secure information dissemination [1], and secure service discovery protocols [2]. In these studies, first an adversary model is defined specifically to the investigated application, then the security mechanism are developed to handle the defined venerabilities, to eliminate threats and to mitigate the risks there.

In our previous work [35] we have presented a secure traffic evaluation protocol (SCOOL). This protocol remarks the security threats of the traffic evaluation protocols on the downtown areas and introduces solutions for each defined vulnerability there. In this paper, we aim to expand our previous work to investigate the vulnerabilities of other traffic efficiency applications on the downtown areas such as: Path recommendations and traffic light controlling mechanisms. Then, a complete secure traffic efficiency control protocol for downtown areas is proposed, we name this protocol by STEP.

3 Adversary Model of The Traffic Efficiency Control Protocols

The traffic efficiency is one of the main categories in the vehicular network applications. Evaluating the real-time traffic characteristics of the road network. Recommending vehicles to follow the most efficient path toward their targeted destinations. Scheduling the located traffic lights according to the real-time traffic distribution on the competing traffic flows. Many other applications have been proposed aiming mainly to increase the traffic fluency and efficiently use the available resources over the road network. All of these applications vitally require the traffic reports of traveling vehicles. Cooperative communications among traveling vehicles and installed road-side units (RSUs) help to gather the real-time traffic characteristics of the investigated area of interest. These traffic characteristics are processed and analyzed to obtain the most efficient recommendations for drivers, traffic lights and other road components. In this section, we discuss three main adversaries on traffic efficiency control protocols.

1) **Integrity**: Aims to ensure that data has not been altered by unauthorized users. It also prevents accidental hold or deletion of data by users. Three main threats can be categorized under this adversary:

   a. *Forgery*: Some drivers alter the reported speed or location of their vehicles. Then, the vital message of evaluating the traffic characteristics of each area of interest carries wrong data. Moreover, vehicles that forward messages toward far areas may also alter and compromise the forwarded messages or initiate a fake report. This causes to generate inaccurate traffic evaluation reports for the road network. Then, it reduces the performance and correctness of the corresponding efficiency control protocol such as efficient path recommendation protocols and intelligent traffic light scheduling algorithms.

   b. *Denial of service*: In this case, attackers forbade the communication channel by overloading it with useless messages. Attackers can use the Botnet system (*i.e.*, set of compromised nodes attack the same target on the computer network). Unexpected large number of fake vehicles asking for recommendations from the same RSU prevent other vehicles from sending their requested information. Several vehicles broadcast large number of messages in a short period of time increases the demand on the communication channels as well. These scenarios negatively affect the performance and accuracy of traffic efficiency application protocols.

c. *Black-hole attack*: Some attackers and malicious vehicles drop all or few selected packets without informing the senders. Then, several packets are lost over the network and will not be considered in the traffic evaluation. Based on the importance and number of the lost packets, this affects the performance of the traffic efficiency control protocols.

2) **Impersonation**: Is used to gain an access to the vehicular network in order to commit fraud or identity theft.

a. *Sybil attacks*: In this attack vehicles broadcast several messages containing different fake identities and locations over a certain area of interest. Then, fake traffic conditions are reported regarding that area of interest. This should affect the traffic efficiency controlling protocols by recommending vehicles to avoid the fake congested area or reschedule the located traffic lights to reduce that fake congestion.

b. *Masquerading*: Some attackers use fake identity that is related to other vehicles or RSUs. These attackers aim at utilizing some facilities and functionalities through legitimate access identification. This can be achieved by spoofing the identity of other nodes or replaying some legal packets (*i.e.*, man-in-the-middle attack).

c. *Non-repudiation*: Some vehicles deny sending or receiving a certain packet over the network. In this case, senders can send a damage data without being asked to take responsibility of sending such data. Moreover, any vehicle can deny receiving some vital packets that it did not obey and then it has caused a chaos on the road network.

3) **Privacy**: Deals with the ability a driver has to determine what data to be shared with third parties. Moreover, if the driver has to reveal his/her identity when sending a message or it can be sent anonymously.

a. *Traceability*: This threat defines the ability of tracing a certain vehicle actions over the network. This includes broadcast messages, request services or reporting cases. Tracing the actions of vehicles on the road network helps to trace their locations and identity.

b. *Linkability*: This refers to the case that an unauthorized entity can link a vehicle identity to its driver/owner. This is introduced for localizing people and tracing their information.

4 The Proposed Secure Traffic Efficiency Control Protocol: STEP

This section presents the details of the proposed Secure Traffic Efficiency control Protocol (STEP). As discussed in Section 2 several protocols were proposed to control traffic efficiency over the road network in the downtown areas. In those protocols, transmitting packets among traveling vehicles (V2V) and transmitting packets between vehicles and installed Road-Side-Units (V2I) have been used to provide real-time and efficient recommendations. Several RSUs are expected to be installed over downtown areas that can help to strength the communications as a backbone to all real-time protocols. In order to secure the traffic efficiency control applications over the downtown areas we propose the STEP protocol.

4.1 Basic Setup of STEP

The STEP protocol provides secure communications among travelling vehicles over downtown areas using the group-based cryptography technique. Vehicles transfer encrypted messages that only targeted receiver/receivers can understand, without the need of revealing the identity or the privacy of any vehicle. In traffic efficiency protocols, each vehicle is interested to transmit messages toward its neighboring vehicles (*i.e.*, same road segment in the downtown). In this work we define the road segment over downtown areas as the road between two adjacent road intersections. Thus, several road segments are configured geographically close each other in order to enhance the management processes there.

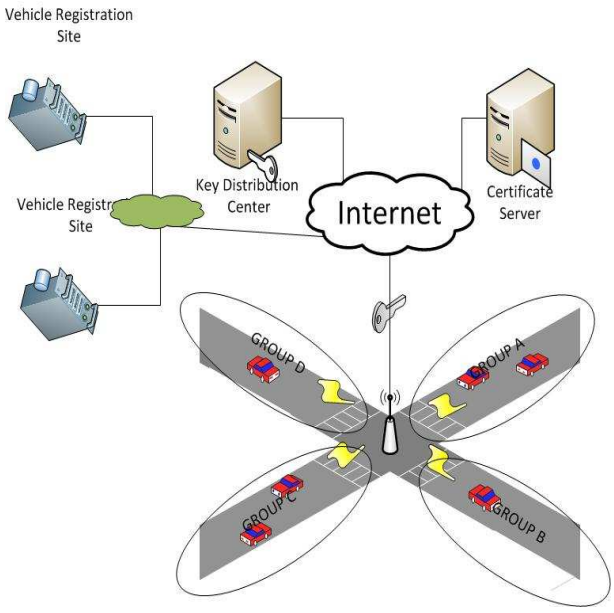


Figure 1: Downtown STEP authentication scenario

The installed RSUs over downtown areas are connected

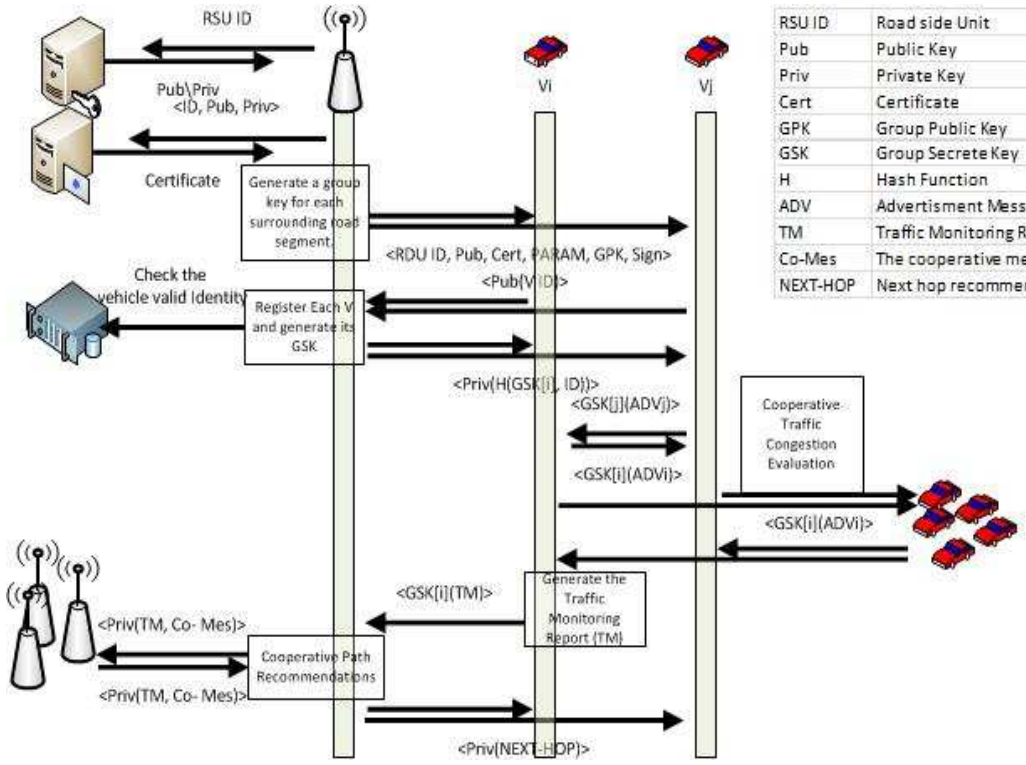


Figure 2: Phases of STEP

to the country vehicles registration authorities. As illustrated in Figure 1 several groups are configured over there. RSUs are responsible of providing each vehicle with the required variables to generate its key at the configured group. Several groups are handled by the same RSU over the road networks, each RSU should be able to prove its identity into vehicles aiming to achieve integrity, authenticity and privacy of communications.

RSUs provide the certificate authorities of vehicles since it is directly connected to vehicles registration authority. Each RSU provides close vehicles with the required variables to generate the group-key at each configured road segment, we assume that each group should be on the same road segment. Each RSU handles several road segments (*i.e.*, several groups) over the downtown scenarios. However, the RSU should be able to prove its identity in order to guarantee the integrity and authenticity of its communications. Each RSU contacts the *Key Distribution Center* to obtain public and private key pair, (Pub_i, $Priv_i$). Moreover, the *Certificate Server* provides the RSU with a certificate that contains: RSU's identity and public key that is encrypted by the Certificate Server's private key. This certificate has an expiration time and they are timestamped to prevent replay attacks. Figure 1 illustrates how RSUs contact with *Key Distribution Center* and *Certificate Server* over downtown areas.

RSUs generate the required bilinear groups with the following road segment parameters: Let $Group_1$ and $Group_2$ be two multiplicative cyclic groups of the same prime order p, gen_1 and gen_2 are generators of $Group_1$ and $Group_2$ respectively. The computable map with the Bilinearity and Nondegeneracy properties is represented by the following relation $e : Group_1 \times Group_2 \rightarrow Group_T$ [19]. ψ is a computable isomorphism from $Group_1$ to $Group_2$, with $\psi(gen_1) = gen_2$. Then, each RSU selects two random elements r and r_0, where $r \in Group_1$ and $r \neq 1_{Group_1}$, $r_0 \in Group_2$ and $r_0 \neq 1_{Group_2}$. That RSU also selects two random numbers $\xi_1, \xi_2 \in Z_q^*$, and sets $u, v \in Group_1$ such that $u^{\xi_1} = v^{\xi_2} = r$ and $r_1, r_2 \in Group_2$ such that $r_1 = {r_0}^{\xi_1}$, $r_2 = {r_0}^{\xi_2}$. The RSU randomly selects $\gamma \in Z_q^*$ as a private key and sets $w = {gen_2}^{\gamma}$ as a system parameter. A secure hash function, $Hash$, is randomly chosen for each road segment too.

The system parameters (PR) after these computations are represented by: $Group_1$, $Group_2$, $Group_T$, gen_1, gen_2, p, ψ, e, $Hash$, w, u, v, r, r_0, r_1, and r_2. The group public key (GPK) is represented by the following parameters: gen_1, gen_2, w. We assume that the Strong Diffie-Hellman (SDH) assumptions hold on $Group_1 and Groip_2$ [6] and the linear Diffie-Hellman assumption hold on $Group_1$ [8].

Each RSU broadcasts an initialization message, I_{messg}, the latter message contains that RSU's *ID, public key and certificate*. It also contains the targeted road segment's *ID*, the system parameters (PR) and group public key GPK. In order to guarantee the integrity, each RSU uses its private key to encrypt the road segment's *ID, PR and GPK* and adds the encrypted data (Enc_{data}) to the I_{messg} message.

Upon receiving any I_{messg}, any traveling vehicle, V_i, first uses the Certificate Server public key to verify the identity and the public key of that RSU. Then, it uses the RSU's public key to verify the integrity of the intended road segment identity and the generated group key. Only if V_i is currently located on the same road segment, it keeps the values of PR and GPK in its database. Consequently, the vehicle, V_i, sends a request message to the RSU aiming to register to that group, where the requested message includes an encrypted value of the real identity ID_i of V_i, using the RSU's public key. The RSU generates a private key $GSK[i]$ for each V_i with its identity. The $GSK[i]$ is represented by (A_i, x_i), where $x_i \leftarrow H(\gamma, ID_i) \in Z_q^*$ and $A_i \leftarrow {g_1}^{1/(\gamma+x_i)}$. It stores (A_i, ID_i) in its database, aiming to guarantee conditional privacy. Then, the RSU uses the secure hash function to encrypt the secrete key of that vehicle, $H(GSK[i], ID_i)$. Finally, it encrypts the hashed value using the RSU's private key and sends it back to the vehicle V_i.

Thus, all RSUs and vehicles obtain their public, group and private keys. Figure 2 illustrates, in details, the sequential steps of the setup phase in a systematic manner.

4.2 Secure Traffic Data Gathering

Each traveling vehicle V_i uses its group key GSK to encrypt the advertisement message, ADV_i. This message is periodically broadcasted to announce the basic traffic data of each vehicle (*i.e.*, ID, location, speed, direction, destination, etc). On the other hand, each vehicle gathers these ADV messages from its neighboring vehicles at the same road segment to predict the traffic situation over that road segment. Vehicles use the group public key, GPK to retrieve the guaranteed basic traffic data of the sender vehicle. In the case any suspicious message is received it can be simply dropped. Only messages that satisfy the security requirements (*i.e.*, retrieve correct data after decrypting by GPK) can be used to evaluate the traffic characteristics on the road network.

The vehicle located in the closest location to the corresponding RSU, V_C, uses the gathered traffic data to generate the traffic monitoring report of that road segment. This report includes: Traffic speed (*i.e.*, average speed of all vehicles), traffic density (*i.e.*, number of vehicles per meter square) and the expected traveling time of that road segment (based of the road segment length and the traffic speed there). V_C sends the traffic monitoring report encrypted by its GSK key. The receiver RSU uses the GPK to verify the identity of the sender vehicle and the correctness of the received data [8].

4.3 Secure Efficient Path Recommendation

Based on the traffic distribution over the road network, the most efficient path toward any targeted destination is configured at each installed RSU. In the case that, vehicles contact the located RSUs with its targeted destinations to request the best path toward their destinations. The requested message is encrypted by the GSK in oder to secure the targeted destination of the vehicle and to guarantee the authenticity. The located RSU uses GPK to read the details of the message. Then, it replies with the best path recommendation message that is encrypted by GPK.

On other cases, when the RSU periodically broadcasts a list of common targeted destinations and the next hop toward each one. In this scenario, the RSU should add a digital signature to the broadcast message to prove the integrity and authenticity of the message. Thus, malicious nodes cannot impersonate RSUs and direct the vehicles falsely.

4.4 Secure Traffic Light Controlling

Intelligent traffic lights are located as RSUs at the road intersections. Each traffic light is provided with wireless transceiver and simple processor. Traffic lights aim to guarantee safe sharing of the road intersections where conflicted flows of traffic can pass the road intersection. The schedule of each intelligent traffic light is set based on the real-time traffic characteristics of the competing flows of traffic. The sequences and the assigned time of each phase are set to minimize the queuing delay time and to increase the throughput of the signalized road intersection.

The traffic characteristics of each flow of traffic that are delivered to the scheduling processor should be encrypted using GSK of the reported vehicle. The receiver processor (RSU) uses the GPK key to verify the correctness of the received data and to verify the identity of the sender. Moreover, the schedule of each traffic light should be encrypted using the private key of the RSU. The receiver vehicles use the public key of the RSU to verify the correctness of the received data. It also checks the identity of the RSU in order to check any fake announced schedule.

5 Performance Evaluation

This section investigates the benefits of the proposed protocol in terms of controlling the traffic efficiency over the road network. This study takes its place in the case that different malicious nodes are existed and transfer fake data aiming to deceive drivers. We compare the performance of the STEP protocol to different traffic controlling protocols, where different number of malicious vehicles were detected.

5.1 Accuracy of Data Gathering

Here, we evaluate the accuracy of the gathered traffic data over the road network. This data is used to control the traffic efficiently. Malicious vehicles broadcast several advertisement messages with different identities and fake basic data. We compare the performance of the STEP protocol to ECODE [34](*i.e.*, one of the traffic evaluation

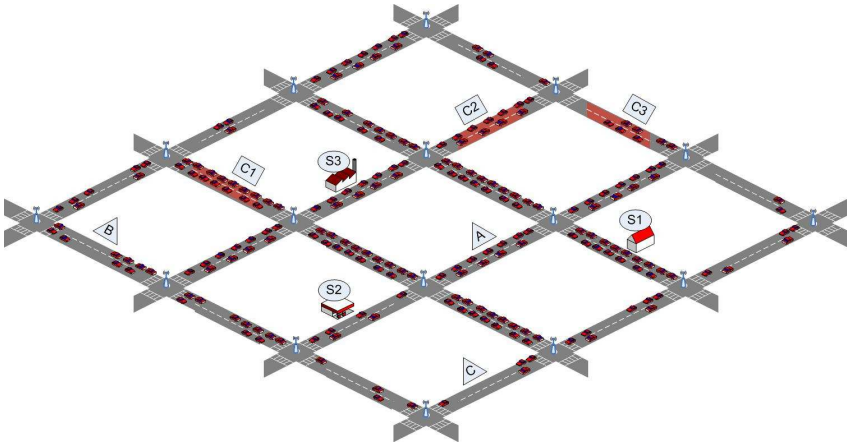


Figure 3: An example of 4X4 manhattan and three targeted destinations (A, B and C)

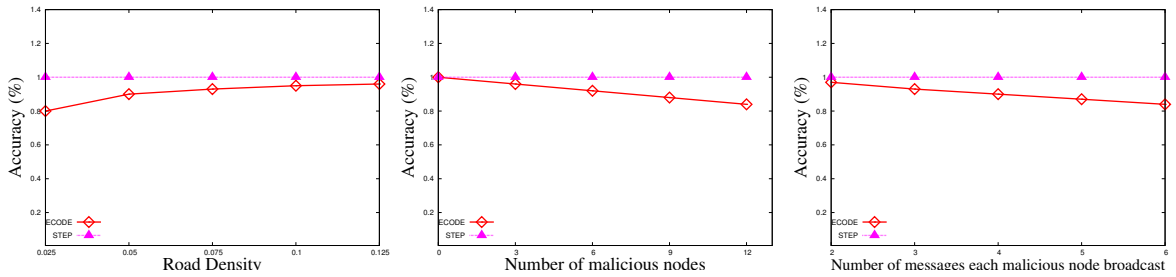


Figure 4: Data gathering accuracy of STEP: (a) Accuracy of STEP compared to ECODE for different traffic densities, (b) Accuracy of STEP compared to ECODE for different number of malicious nodes and (c) Accuracy of STEP compared to ECODE when each malicious node send different number of advertisement messages

protocols for road networks) in term of the accuracy of data gathering. We measure the accuracy of each protocol by comparing the number of detected vehicles to the number of existed vehicles over each road segment. Table 3 illustrates the simulation parameters of the performance comparison.

Table 1: Simulation parameters

Parameter	**Value**
Simulator	NS-2, SUMO
Transmission range (m)	250
Simulation time (s)	2000
Simulation area (m^2)	20 X 200
Number of Vehicles	20 - 100
Simulation map	2 lane road segment
Traffic speed	1-10 m/s
Mobility model	downtown mobility
Number of malicious nodes	4-12
Number of fake messages	2-5

In Figure 4, the comparative results of the data gathering accuracy for STEP and ECODE protocols are presented. First, in Figure 4(a) we assume the existence of five malicious nodes each one broadcast five advertisement messages. From this figure we can infer that the importance of securing the data gathering protocols is increased when the traffic density is less over the road network. By increasing the traffic density while the same number of malicious nodes are existed the effect of these nodes is becoming negligible regarding the traffic evaluation.

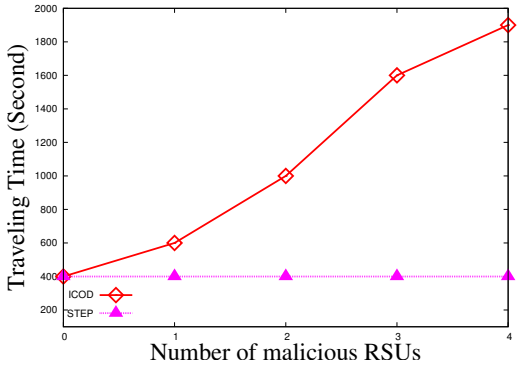
Second, we study the effect of increasing the number of malicious nodes over the road scenario where the traffic density is fixed to 0.075 $vehicle/meter^2$. The results of comparison is illustrated in Figure 4(b), several malicious nodes are simulated where each node broadcast five advertisement messages. From Figure 4(b) we can clearly see that by increasing the number of the malicious nodes the accuracy of traffic evaluation is decreased without using the secure protocol.

Figure 4(c) investigates the effect of the number of advertisement messages that each malicious node send. The malicious node becomes more disturbing when it broadcasts more fake messages in ECODE. Figure 4(a), Figure 4(b) and Figure 4(c) have shown that the STEP protocol can detect all fake messages broadcast by malicious nodes. Thus, it is able to produce accurate traffic evaluation.

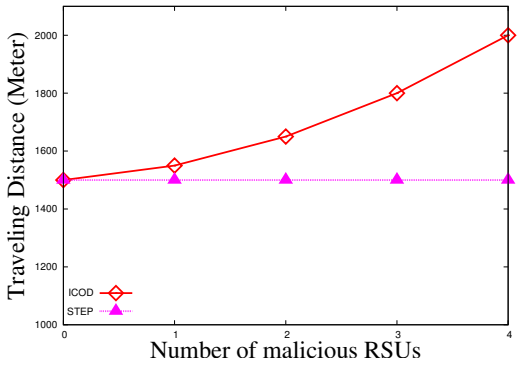
Table 2: Simulation parameters

Parameter	Value
Simulator	NS-2, SUMO
Transmission range (m)	250
Simulation time (s)	2000
Simulation area (m^2)	1000 X 1000
Number of vehicles	200 - 1000
Simulation map	Grid-layout
Mobility model	downtown mobility
Traffic speed	1-10 m/s
Number of malicious RSUs	0-4

5.2 Efficiency of The Configured Path



(a)



(b)

Figure 5: Efficiency of STEP compared to ICOD: (a) Traveling time of the configured path, (b) Traveling distance of the configured path

In this section we investigate the effects of the existence of some malicious RSUs on the road network in terms of configuring the efficient path toward targeted destinations. We run our experiments in 4X4 Manhattan model 16 RSUs are expected to be installed one at each intersection. We assume that all drivers on this road network are targeting one of three destinations, A, B and C, as illustrated in Figure 3. Some road segments are highly congested while others witness a low traffic density. Malicious RSUs broadcast fake and in-accurate data about one of the targeted destinations, drivers will be deceived to travel more time and extra distance then. Table 2 illustrates the simulation parameters for this comparison experiment.

We compare the performance of the STEP protocol in terms of configuring efficient path to ICOD [38] one of the distributed path recommendation protocols. Figure 5 illustrates the comparison study between these protocols. In Figure 5(a) we can see that by increasing number of malicious RSUs over the road network, the average traveling time toward these destinations is increased drastically by ICOD. This is due to recommending the highly congested road segments on the road network in these cases. At the same time Figure 5(b), the average traveling distance is increased when using ICOD to configure the efficient paths. However the increased in the traveling distance is small compared to the increase in the traveling time, this can be clearly seen from Figure 5(a) and Figure 5(b). The STEP protocol was able to configure malicious RSUs and ignore the recommendation messages they broadcast. Thus, the STEP protocol acquire better traveling time and traveling distance regardless of the number of existed malicious RSUs.

5.3 Efficiency of The Traffic Light Schedule

Table 3: Simulation parameters of ITLC

Parameter	Value
Simulator	NS-2 , SUMO
Transmission range (m)	250
Simulation time (s)	2000
Simulation area (m^2)	1000 X 1000
Number of traffic lights	1
Number of vehicles	200 - 1000
Simulation map	4-leg traffic intersection
Mobility model	downtown mobility
Number of malicious RSUs	0-4

We measure the efficiency of the traffic light schedule by the average waiting delay time of each vehicle at the traffic light and the throughput of the signalized road intersection (*i.e.*, number of vehicles passing the intersection per second). Malicious drivers can deceive the traffic light by broadcasting several advertisement messages to increase the traffic density of the traffic flow. Moreover, they can announce themselves as emergency vehicles that have a higher priority to pass the signalized intersection first. This drastically decrease the efficiency performance of the traffic light schedule. Figure 6 compares the STEP protocol to ITLC [36] in term of efficiency of the traffic light schedule. The average waiting delay of each vehicle is illustrated in Figure 6(a). As we can see from this figure by increasing the number of malicious drivers at the signalized intersection, the waiting delay time of each vehicle is increased when using the ITLC protocol. On the other hand, Figure 6(b) shows that using ITLC protocol to gen-

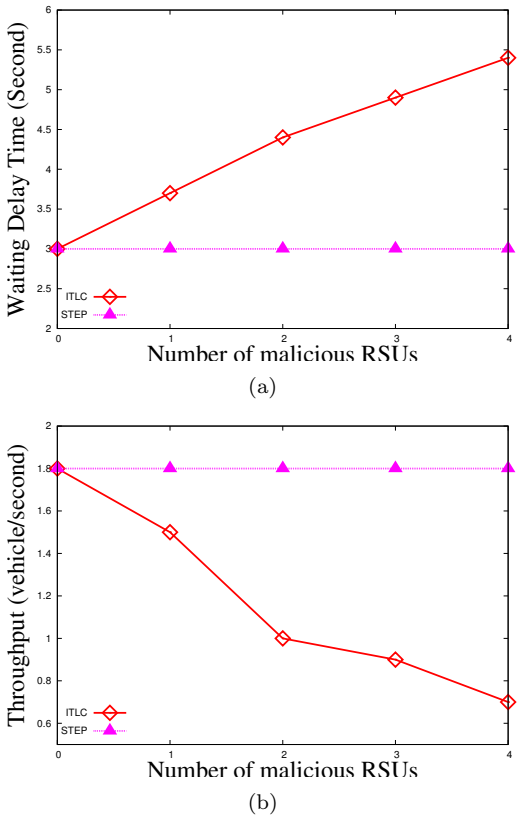


Figure 6: The efficiency of traffic light schedule: (a) Average waiting delay of each vehicle, (b) Throughput of the signalized intersection

erate the schedule of the traffic light, the throughput of the signalized intersection is decreased.

6 Conclusions

In this paper, we have proposed a secure traffic congestion control protocol, STEP. This protocol controls the traffic congestion problem over the downtown areas in a secure and efficient fashion. It relays on the public cryptography to authenticate RSUs at road intersections. On the other hand, at each road segment the group signature is used to secure the communications between vehicles. Experimental results have indicated that the efficiency protocols achieves better performance in the case that secure communications are used. This is due to the behavior of the malicious nodes which intend to deceive the efficiency control protocols aiming to serve their benefits.

References

[1] K. Abrougui and A. Boukerche, "An efficient secure service discovery protocol for intelligent transportation systems," in *IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'11)*, pp. 756–760, 2011.

[2] K. Abrougui, A. Boukerche, and Y. Wang, "Secure gateway localization and communication system for vehicular ad hoc networks," in *IEEE Global Communications Conference (GLOBECOM'12)*, pp. 391–396, 2012.

[3] O. Abumansoor and A. Boukerche, "A secure cooperative approach for nonline-of-sight location verification in vanet," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 275–285, 2012.

[4] Q. A. Arain, D. Zhongliang, I. Memon, S. Arain, F. K. Shaikh, A. Zubedi, M. A. Unar, A. Ashraf, and R. Shaikh, "Privacy preserving dynamic pseudonym-based multiple mix-zones authentication protocol over road networks," *Wireless Personal Communications*, vol. 95, no. 2, pp. 505–521, 2017.

[5] C. T. Barba, M. A. Mateos, P. R. Soto, A. M. Mezher, and M. A. Igartua, "Smart city for vanets using warning messages, traffic statistics and intelligent traffic lights," in *IEEE Intelligent Vehicles Symposium (IV'12)*, pp. 902–907 , 2012.

[6] N. Barić and B. Pfitzmann, "Collision-free accumulators and fail-stop signature schemes without trees," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 480–494, 1997.

[7] P. Bellavista, F. Caselli, A. Corradi, and L. Foschini, "Cooperative vehicular traffic monitoring in realistic low penetration scenarios: The colombo experience," *Sensors*, vol. 18, no. 3, pp. 822, 2018.

[8] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Annual International Cryptology Conference*, pp. 41–55, 2004.

[9] W. Chen and Y. Sun, "On the security cost of interval multicast," in *International Conference on Information and Automation (ICIA'09)*, pp. 101–105 , 2009.

[10] M. S. Hwang C. Y. Tsai, P. F. Ho, "A secure group signature scheme," *International Journal of Network Security*, vol. 20, no. 2, pp. 201–205, 2018.

[11] L. D. Chou, D. C. Li, and H. W. Chao, "Mitigate traffic congestion with virtual data sink based information dissemination in intelligent transportation system," in *Third International Conference on Ubiquitous and Future Networks (ICUFN'11)*, pp. 37–42 , 2011.

[12] E. C. Eze, S. J. Zhang, E. J. Liu, and J. C. Eze, "Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development," *International Journal of Automation and Computing*, vol. 13, no. 1, pp. 1–18, 2016.

[13] J. Fukumoto, N. Sirokane, Y. Ishikawa, T. Wada, K. Ohtsuki, and H. Okada, "Analytic method for real-time traffic problems by using contents oriented communications in vanet," in *7th International Conference on ITS Telecommunications (ITST'07)*, pp. 1–6 , 2007.

[14] R. L. Gordon, W. Tighe, ITS Siemens, *et al.*, Traffic Control Systems Handbook, FHWA-HOP-06-006, 2005.

[15] V. Gradinescu, C. Gorgorin, R. Diaconescu, V. Cristea, and L. Iftode, "Adaptive traffic lights using car-to-car communication," in *65th Vehicular Technology Conference (VTC'07)*, pp. 21–25, 2007.

[16] D. Greenwood, B. Burdiliak, I. Trencansky, H. Armbruster, and C. Dannegger, "Greenwave distributed traffic intersection control," in *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 2*, pp. 1413–1414, 2009.

[17] W. J. Hu, Y. B. Huang, Q. Y. Zhang, "Robust speech perception hashing authentication algorithm based on spectral subtraction and multi-feature tensor," *International Journal of Network Security*, vol. 20, no. 2, pp. 206–216, 2018.

[18] C. T. Li, M. S. Hwang, Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks", *Computer Communications*, vol. 31, no. 12, pp. 2803-2814, July 2008.

[19] X. Lin, X. Sun, P. H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[20] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "Uav-enabled intelligent transportation systems for the smart city: Applications and challenges," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 22–28, 2017.

[21] K. Nellore and G. P. Hancke, "A survey on urban traffic management system using wireless sensor networks," *Sensors*, vol. 16, no. 2, pp. 157, 2016.

[22] Z. Ozcelik, C. Tastimur, M. Karakose, and E. Akin, "A vision based traffic light detection and recognition approach for intelligent vehicles," in *International Conference on Computer Science and Engineering (UBMK'17)*, pp. 424–429 , 2017.

[23] K. Pandit, D. Ghosal, H. M. Zhang, and C. N. Chuah, "Adaptive traffic signal control with vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1459–1471, 2013.

[24] K. Pandit, D. Ghosal, H. M. Zhang, and C. N. Chuah, "Adaptive traffic signal control with vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1459–1471, 2013.

[25] J. Qian and R. Eglese, "Fuel emissions optimization in vehicle routing problems with time-varying speeds," *European Journal of Operational Research*, vol. 248, no. 3, pp. 840–848, 2016.

[26] M. Riley, K. Akkaya, and K. Fong, "Group-based hybrid authentication scheme for cooperative collision warnings in vanets," *Security and Communication Networks*, vol. 4, no. 12, pp. 1469–1482, 2011.

[27] M. A. Salman, S. Ozdemir, and F. V. Celebi, "Fuzzy logic based traffic surveillance system using cooperative v2x protocols with low penetration rate," in *International Symposium on Networks, Computers and Communications (ISNCC'17)*, pp. 1–6 , 2017.

[28] M. Sankaranarayanan, C. Mala, and S. Mathew, "Congestion rate estimation for vanet infrastructure using fuzzy logic," in *Proceedings of the International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence*, pp. 98–102, 2017.

[29] O. Tomescu, I. M. Moise, A. E. Stanciu, and I. Batros, "Adaptive traffic light control system using ad hoc vehicular communications network," *UPB Scientific Bulletin, Series D*, vol. 74, no. 2, 2012.

[30] K. Upasani, M. Bakshi, V. Pandhare, and B. K. Lad, "Distributed maintenance planning in manufacturing industries," *Computers & Industrial Engineering*, vol. 108, pp. 1–14, 2017.

[31] C. Vilarinho, J. P. Tavares, and R. J. F. Rossetti, "Intelligent traffic lights: Green time period negotiaton," *Transportation Research Procedia*, vol. 22, pp. 325–334, 2017.

[32] M. B. Younes, G. R. Alonso, and A. Boukerche, "A distributed infrastructure-based congestion avoidance protocol for vehicular ad hoc networks," in *IEEE Global Communications Conference (GLOBECOM'12)*, pp. 73–78 , 2012.

[33] M. B. Younes and A. Boukerche, "A performance evaluation of a context-aware path recommendation protocol for vehicular ad-hoc networks," in *IEEE Global Communications Conference (GLOBECOM'13)*, pp. 516–521 , 2013.

[34] M. B. Younes and A. Boukerche, "A performance evaluation of an efficient traffic congestion detection protocol (ECODE) for intelligent transportation systems," *Ad Hoc Networks*, vol. 24, pp. 317–336, 2015.

[35] M. B. Younes and A. Boukerche, "Scool: A secure traffic congestion control protocol for vanets," in *IEEE Wireless Communications and Networking Conference (WCNC'15)*, pp. 1960–1965 , 2015.

[36] M. B. Younes and A. Boukerche, "Intelligent traffic light controlling algorithms using vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 5887–5899, 2016.

[37] M. B. Younes and A. Boukerche, "An efficient dynamic traffic light scheduling algorithm considering emergency vehicles for intelligent transportation systems," *Wireless Networks*, pp. 1–13, 2017.

[38] M. B. Younes, A. Boukerche, and G. Rom'an-Alonso, "An intelligent path recommendation protocol (icod) for vanets," *Computer Networks*, vol. 64, pp. 225–242, 2014.

[39] M. B. Younes, A. Boukerche, and X. Zhou, "An intelligent vehicular traffic prediction (itp) protocol," in *IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, pp. 899–904, 2015.

[40] X. Zhang, V. J. Karplus, T. Qi, D. Zhang, and J. He, "Carbon emissions in china: How far can new efforts bend the curve?," *Energy Economics*, vol. 54, pp. 388–395, 2016.

[41] J. Zhong and H. Liao, "Research on the applications of electronic information technology in intelligent

traffic light signal control," in *Proceedings of International Conference on Computing,Communications and Automation (I3CA'17)*, 2017.

[42] S. Zhong, X. Xiao, M. Bushell, and H. Sun, "Optimal road congestion pricing for both traffic efficiency and safety under demand uncertainty," *Journal of Transportation Engineering, Part A: Systems*, vol. 143, no. 4, pp. 04017004, 2017.

Biography

Maram Bani Younes received the Ph. D. degree in computer science from the University of Ottawa, Ottawa, ON, Canada, in 2015. She is currently an Assistant Professor with the Department of Computer Science, Philadelphia University, Jordan, and a Research Associate with the School of Information Technology and Engineering, University of Ottawa. Her research interests are wireless networks, wireless ad hoc and sensor networks, vehicular networks and traffic efficiency for vehicular network.