Reliable and Secure Distributed Smart Road Pricing System for Smart Cities

Siham Bouchelaghem and Mawloud Omar

***Abstract*—Vehicular networks have emerged as a promising technology for the development of traffic management systems in smart cities. They are expected to revolutionize a variety of applications such as traffic monitoring and pay-as-you-drive services. Recently, the notion of road pricing has become crucial in most big cities as it contributes in road congestion avoidance, fuel consumption saving and pollution reduction. However, as the road pricing systems need trip data to invoice citizens, it is vital to ensure geolocation privacy while keeping drivers honest. In this paper, we propose a security approach for Smart Road Pricing (SRP) systems, which prevents toll evasion violations. The proposed approach operates under a fully distributed threshold-based control system to detect fraudulent drivers trying to cheat on their tolls. The accused drivers are reported to the toll server in order to take the appropriate countermeasures. Through the security analysis, we show the robustness of the proposed approach against a range of potential attacks. We also evaluate the proposed approach through simulations considering important metrics, namely, the storage and communication overheads. The proposed approach shows better performance results in comparison to the existing approaches. Furthermore, we evaluate the proposed approach efficiency in terms of detection precision, where it demonstrates promising results.**

***Index Terms*—Vehicular networks, Smart cities, SRP, Toll evasion, Security.**

I. Introduction

VEHICULAR networks play a key role in the design of traffic management systems in smart cities [2], [3], [8]. They are considered as a promising technology for traffic data collection that facilitate road efficiency and safety applications through Intelligent Transportation Systems (ITS). In fact, the increasing number of vehicles on the roads in big cities has risen many challenges for the authorities concerning traffic congestion, road accidents and health hazards. To cope with these issues, cities around the world are focusing their efforts on using advanced and innovative technologies to make their traffic management systems ”smarter” [13].

Road pricing has emerged as an effective approach to reduce bottlenecks, encourage carpooling and traveling in public transport, and ensure only unavoidable journeys on the most congested roads. Current Electronic Road Pricing (ERP) systems require gantries located along highways and roads to reduce congestion during peak hours, as well as In-vehicle Units (IU) that are affixed on every vehicle [5]. The system also relies on Radio Frequency Identification (RFID) to charge drivers using smart cards inserted into the IUs each time their vehicle passes under a gantry. Recently, smart cities tend to evolve the existing ERP into Smart Road Pricing (SRP) systems. This new generation of ERP relies on Global Navigation Satellite System (GNSS) technology instead of the usual physical gantries freeing up road space and reducing maintenance costs [4]. The SRP system uses satellites to determine when a vehicle enters a toll road to charge tolls to citizens accounts directly according to the public charging policy. However, security in the SRP systems is an important challenge, which should be addressed since dishonest users, with the aim to pay less, tend to cheat on their tolls. Moreover, citizens are increasingly worried about deliberate surveillance and potential breach of privacy. In fact, the probability of fraud in current ERP systems is minimal since the gantries located in toll roads and highways are equipped with cameras, which photograph all the vehicles passing through the gantries. Therefore, in case of a toll evasion violation, photographs of the vehicles license plates, captured by the enforcement camera system are used to send a violation notice to the registered owner of the vehicle. However, the probability of fraud in SRP systems is more significant as each vehicle traveling on a toll road reports its own geolocation to the toll server. Given the increased risk of fraud, the addressed problem in this paper aims to minimize any overhead of costly technologies in terms of hardware. In fact, the main challenge is to develop an effective solution for toll fraud actions detection, while eliminating any additional equipment (e.g., cameras) that highly costs in terms of deployment and maintenance, and may lead to citizens privacy breach. Hence, our work uses the recent communication abilities of new generation vehicles to propose a fully autonomous and distributed solution for toll fraud detection. In this context, several solutions for toll evasion have been proposed in the literature. Most of the existing solutions are based on cryptographic mechanisms that impose high computation and communication overheads, which is unfit for vehicular networks. Besides, to prevent dishonest users from cheating, the system uses random spot checks with hidden roadside cameras to observe some of their geolocations for which they will be challenged later. However, deploying too many cameras in the city may lead to citizens privacy violation and thus decrease the public acceptance of SRP systems.

In this paper, we address the issue of fraud detection in SRP systems by the proposition of a comprehensive approach aiming to prevent toll evasion violations. Unlike the solutions proposed in the literature, the proposed approach allows to detect instantly any fraudulent driver trying to cheat on his tolls. Moreover, the operations are performed in a decentralized

S. Bouchelaghem and M. Omar are with Laboratoire d’Informatique Médicale, Faculté des Sciences Exactes, Université de Bejaia, 06000 Bejaia, Algérie.

manner, where the vehicles are involved in the detection of toll fraudulent actions. The proposed approach operates under four components, namely, (1) the system bootstrapping, (2) the threshold-based control system, (3) the fraudulent evidences signature and verification, and (4) the tolling bill management. The detection process makes use of the vehicles collaboration to spot a fraudulent driver trying to cheat on his whereabouts. In this context, undeniable evidences are preserved against such drivers and transmitted to the toll server. With the aim to evaluate the performances of the proposed approach, we have developed simulations, which we have compared to the reviewed approaches. The obtained results are encouraging, in which the proposed approach demonstrates better performances in terms of robustness, storage and communication overheads.

The contribution of this paper is quadruple:

(1) We propose a novel technique of driver fraudulent detection even if the driver disables completely the On-Board Unit (OBU) from its vehicle. In this context, a dynamic and fully distributed threshold-based control system is proposed to share among drivers the ability to cosign the fraudulent evidences and hence dealing against false alerts.
(2) We propose an approach of group formation setting based on relevant criteria, namely, the similarity degree in terms of itinerary, speed and trustworthy. This solution maximizes the group lifetime by allowing the selection of honest driver coalitions such, they remain as long as possible adjacent during the trips.
(3) We investigate the electronic tolling bill format by addressing the case of fraudulent actions. In this context, an approach of tolling bill signature and verification is designed.
(4) The proposed approach is practical and operates with a lightweight load of storage and communication, while providing the important security characteristics such as impersonation attack resistance, privacy, collusion resistance, accountability, confidentiality and unforgeability.

The rest of the paper is organized as follows. In Section II, we review from the literature the solutions designed for fraud detection in SRP systems. In Section III, we introduce a brief background of some cryptographic primitives. In Section IV, we present the detailed description of the proposed approach. In Section V, we analyze the security of the proposed approach, and in Section VI, we evaluate its efficiency through simulations. Finally, we conclude the paper in Section VII.

II. Related work

Over the last few years, several solutions have been proposed to meet the security requirements in SRP systems. In this section, we review and compare some recent and relevant approaches. The latter can be classified based on whether the location data are collected by an external server, property of the Toll Service Provider (TSP), or stored by the OBU.

In the former category, the geolocation data collected by the toll server are anonymized, which results in less computational overheads on the OBU. Moreover, it allows the authorities to use these records for other types of applications such as road traffic monitoring. This type of solutions ignores though the threats that can occur after the user payment information has been computed. An external attacker having access to this information would endanger user geolocation privacy [16]. For instance, Popa et al. [21] have proposed VPriv (protecting PRIVacy in location-based vehicular services), a system that can be used in several location-based vehicular applications including SRP systems. VPriv lies on homomorphic commitments to prove that the users always pay the right amount of tolls for their road usage. It employs also random spot checks with hidden cameras to prevent dishonest drivers from cheating on their geolocations. However, as the users communicate detailed information about their trips, VPriv needs an anonymizing network such as Tor [10], and hence, imposing additional overhead to the system. Chen et al. [17] have proposed the integration of a group signature scheme [25] to guarantee the drivers honesty while preserving their anonymity. In fact, each driver can sign his geolocation information on behalf of the group he belongs to. Later, the toll server can verify the signature using the group public key while the identity of the signer remains secret. However, conditional unlinkability of such schemes ensures that the actual signer can be found in case of fraudulent action detection. Moreover, by organizing the users into groups according to the driving pattern, the system improves the protection of users privacy and prevents an attacker from obtaining their trips history. It is though essential to design a group management policy, which considers emergent situations that might imperil citizens privacy.

Where the geolocation records are stored into the OBU, this offers better protection of drivers privacy but requires the use of cryptographic proofs to demonstrate the OBU honesty in the fee calculation, which imposes heavy computational load to the user devices. To address the shortcomings of VPriv, Balasch et al. [20] have proposed PrETP (PRivacy-preserving Electronic Toll Pricing), where drivers commit to the road segments they drove, revealing no information about their geolocations to the toll server. The system is thus dispensed from the anonymizing network. However, in both VPriv and PrETP systems, the spot checks camera locations are revealed to each driver to verify the veracity of the committed values. This disclosure allows colluding drivers to map and share the cameras locations and reduces their final payment by taking camera-free paths. Meiklejohn et al. [18] have proposed Milo, a system based on PrETP that considers this sort of collusion. Using blind identity-based encryption [23], Milo strengthens the spot checks in PrETP and ensures that the road segments of users can be verified, while guaranteeing that drivers do not learn where they were seen. Troncoso et al. [19] have proposed PriPAYD, a privacy-friendly Pay-As-You-Drive scheme, where the user insurance is bound to the roads he travels. The premium calculations are done locally in the OBU, and only aggregated data necessary to users invoicing are sent to the insurance company to avoid serious privacy breach.

Recently, Jardi-Cedo et al. [9] have proposed a privacy-preserving ERP system for multifare Low Emission Zones (LEZs), where the geolocation data are neither sent to an

external server nor stored into the OBU. The system relies on checkpoints equipped with cameras to control the vehicles access to LEZs. In fact, the system requires a vehicle to authenticate each time it enters, changes or leaves a zone, imposing high communication overhead. Unlike the systems [18], [20], [21], the checkpoints photograph fraudulent drivers only, keeping thus honest drivers privacy. Moreover, all the changes that occur when using different road zones are registered to obtain the final amount to pay.

In Table I, we summarize the main characteristics of each approach. For more details about a particular solution, kindly refer to its corresponding reference.

III. Cryptographic background

In this section, we present some useful notions about digital signature, threshold and elliptic curve cryptography.

A. Digital signature

Digital signature [24] is a cryptographic primitive that aims to protect a message from unauthorized modification, authenticate the sender and prevent it from denying to have signed the message. Given a message m and a private key $\widehat{K}$, the function $\mathcal{S}(m, \widehat{K})$ outputs σ_m, which is the signature for the message m by the private key $\widehat{K}$. A digital signature is correct if for the signature σ_m produced by $\mathcal{S}(m, \widehat{K})$, then the verification function $\mathcal{V}(m, \sigma_m, K)$ is valid, where K is the corresponding public key of $\widehat{K}$.

B. Threshold cryptography

The idea of $\langle t, n\rangle$ based threshold cryptography was introduced by Shamir in [26]. The threshold cryptography is a secret sharing technique that distributes a secret S among n participants in such a way any t of them can reconstruct the secret. However, any $t-1$ or fewer participants can gain no information about S. The threshold cryptography has found applications in many fields including digital signatures, where the key number can be significantly reduced when a group of n participants is involved. In fact, a private key can be divided among the n participants into pieces, called "shares", while in verification only a single public key is needed for the whole group. The signature process can be performed only when t participants of the group are present.

C. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) [6] is most commonly used for encryption, key exchange with Diffie-Hellman protocol and for digital signatures. Given an elliptic curve E over a finite field F_p and a base point Q. A sender Alice encodes any message m as a point P_m on the elliptic curve. Then, she encrypts P_m by computing C_1 and C_2 such as

$$C_1 = P_m + k \cdot K_B, \tag{1}$$

and

$$C_2 = k \cdot Q, \tag{2}$$

where k is a randomly selected integer and K_B is the public key of Bob. Finally, Alice sends $\langle C_1, C_2\rangle$ to Bob, who uses his private key $\widehat{K}_B$ to recover the message m. To do this, he computes

$$P_m = C_1 - \widehat{K}_B \cdot C_2. \tag{3}$$

Since its apparition, ECC has evolved as an attractive alternative to other public key schemes such as RSA. It offers smaller key sizes with equivalent security strength as it relies on the difficulty to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP). The use of ECC is being extended to a wide range of modern applications such as securing vehicular communications in smart cities [11].

IV. The proposed approach

In this section, we present the system model and detail the proposed approach operations.

A. System model

We consider a vehicular network designed for SRP, where each vehicle is equipped with an OBU able to geolocalize itself through GPS (Global Positioning System). The communication that takes place between the vehicles is named Vehicle-to-Vehicle (V2V) communication by using the OBU. Each vehicle is equipped with a stereo camera and a radar to detect around itself the presence or not of adjacent vehicles. At each time a vehicle enters a toll road, the OBU communicates its geolocation to the toll server over its neighboring Road-Side Unit (RSU). To be best suited with regard of several applications, the proposed solution disregards the choice of communication technologies used by OBUs and RSUs. At the end of each pricing period, the drivers have to pay tolls according to a predefined charging policy. In Fig. 2, we illustrate the targeted SRP system architecture.

We consider a threat model, where a fraudulent driver eager to save illegally fees tends to cheat on the information which he delivers about his trips. To do this, he may either cheat on his geolocation or disable the OBU system from his vehicle. In the other hand, a compromised vehicle can eavesdrop the network and tries to impersonate others with which it aims to have the driver trips paid. As the toll server is likely to belong to a governmental organization, we treat it as an honest party, which does not use drivers geolocation records for unwarranted surveillance and traceability. However, the SRP system still raises some privacy concerns as an external attacker may try to eavesdrop the network exchanged messages. Then, it may process the geolocation records to infer sensitive information such as a given home address or work place, or analyze the mobility pattern to profile the drivers (visited places, driving pattern, etc.). Finally, we note that the physical attacks, where a compromised party gain physical access to the OBU of vehicles are out of scope. The main operations of the proposed approach are outlined in the flowchart of Fig. 1. In Table II, we summarize the main used notations and in the following sub-sections, we describe the detailed operations.

TABLE I: Overall comparison of the reviewed approaches

	[21]	[17]	[20]	[18]	[19]	[9]
Location records collected by	Server	Server	OBU	OBU	OBU	Not required
Toll elaboration performed by	Server	OBU	OBU	OBU	OBU	OBU
Dispute solved by	TSP	Authority	TSP	Authority	TSP	Not required
Spot check camera required	Yes	No	Yes	Yes	No	Yes

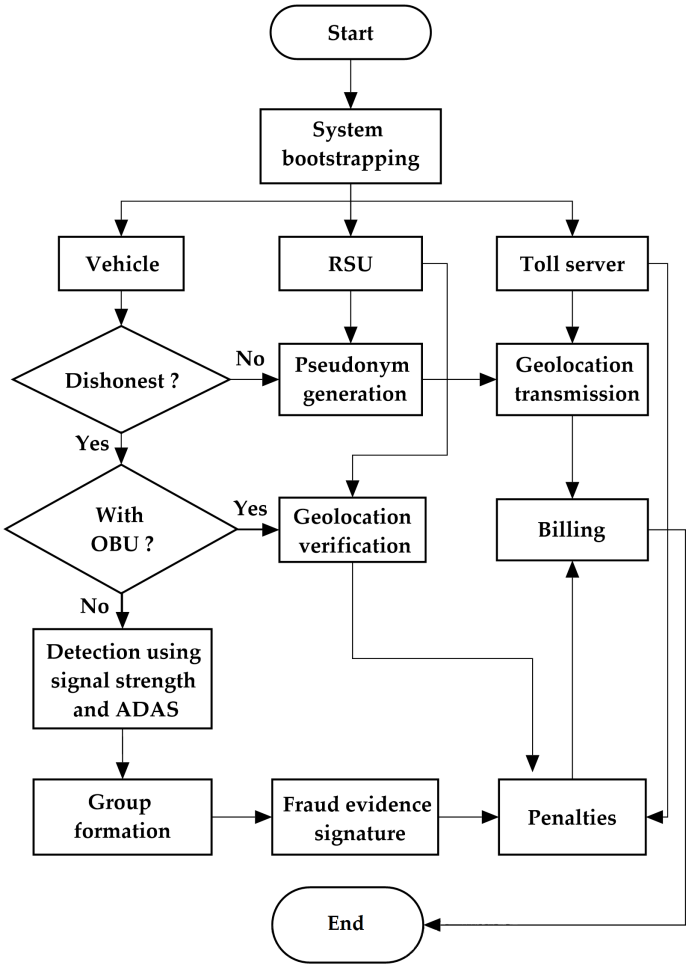

Fig. 1: Flowchart of the proposed approach

TABLE II: Notations

Notation	Description
v_i	Vehicle of identity i
d_i	Vehicle v_i driver
P_i	Vehicle v_i pseudonym
K_i, $\widehat{K}_i$	Vehicle v_i public and private keys
$K_V^{(i)}$, $\widehat{K}_V^{(i)}$	Vehicle v_i public and private shares
$K_S, \widehat{K}_S$	Toll server public and private keys
$\mathcal{B}_i$	Driver d_i tolling bill
$\sigma_{\mathcal{B}_i}$	Driver d_i tolling bill digital signature
$\mathcal{C}_i$	Driver d_i tolling bill amount
f	Fee policy function
$\langle L_i^l, T_i^l \rangle$	l^{th} tuple of vehicle v_i geolocations
$\langle t, n \rangle$	Threshold control system scheme
V	Threshold control system group
$K_V, \widehat{K}_V$	Group V public and private keys
$\mathcal{F}$	Group formation objective function
$\mathcal{R}$	Degree of resemblance
α, β and γ	Function $\mathcal{F}$ metric coefficients
I_{ij}	Itinerary similarity rate of v_i and v_j
S_{ij}	Speed similarity rate of v_i and v_j
R_{ij}	Reputation correspondence of v_i and v_j
ℓ_i	Shared secret between the RSU and v_i
D_{ij}	Cartesian distance between v_i and v_j
s_i	Vehicle v_i partial signature
$\mathcal{E}_k$	Fraudulent action evidence against v_k
$\mathcal{H}$	Collision-resistant hash function
F_p	Finite field of cardinal p
$E_p(a, b)$	Elliptic curve over F_p
Q	Base point on the elliptic curve
q	Large prime number

B. System bootstrapping

To get access to the SRP system, some parameters should be stored into the OBU of vehicles. For instance, each vehicle v_i will have a unique value to identify itself to the toll server. Besides, as the OBU will have to verify the tolling bill signature at the end of each pricing period, it stores the toll server public key K_S. It will also need to generate a key pair $\langle K_i, \widehat{K}_i \rangle$, where the public key K_i is bound to its identifier and shared with the toll server, while the private key $\widehat{K}_i$ is kept secret.

During driving and upon entering a toll road, each vehicle sends its geolocation to the toll server. Before starting the tolling process, each vehicle generates a pseudonym. The latter is used to send anonymously the geolocation and time information, and later, for any V2V communication along the toll road. The pseudonym generation is performed as follows.

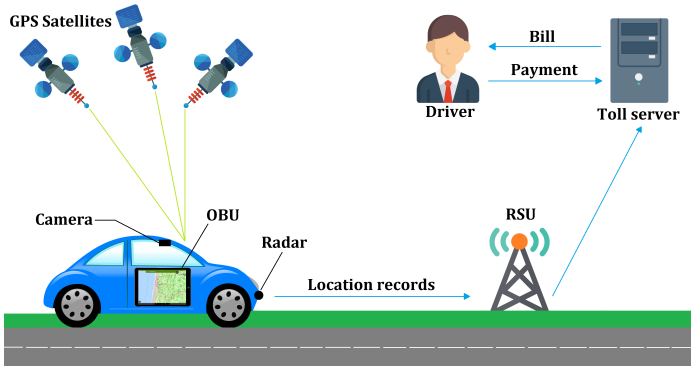

Fig. 2: SRP system architecture

Let's consider a vehicle v_i being in a given geolocation L_i at a given time T_i, and a RSU within its communication range. Each one of them should be aware of its interlocutor public key in order to generate securely the vehicle v_i pseudonym. The OBU and RSU exchange their respective public keys K_i and K_{RSU}, which are used to compute a shared Diffie-Helman-based secret ℓ_i such as

$$\ell_i = (x_{\ell_i}, y_{\ell_i}) = \widehat{K}_i \cdot K_{RSU} = \widehat{K}_{RSU} \cdot K_i, \tag{4}$$

where x_{ℓ_i} and y_{ℓ_i} are respectively the x and y coordinates of the point ℓ_i. Afterwards, both of OBU and RSU compute the vehicle v_i pseudonym P_i such as

$$P_i = \mathcal{H}(x_{\ell_i}||i||ID_{RSU}||L_i||T_i), \tag{5}$$

where $\mathcal{H}$ is a collision-resistant hash function. Finally, the RSU broadcasts $\langle i, P_i, T_i \rangle$ to its neighboring RSUs over a secure communication channel.

C. Threshold-based control system

Let's consider the scenario illustrated in Fig. 3, where three vehicles v_i, v_j and v_k move on a toll road. We assume that the vehicles v_i and v_j are honest, while v_k is dishonest and tries to cheat on his geolocation to avoid paying the road usage. To do this, the vehicle v_k should either give a false information about its geolocation or the driver completely disables the OBU by putting it out of the power.

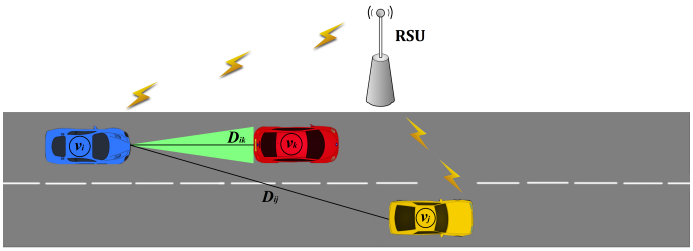

Fig. 3: Dishonest vehicle identification

In the first scenario, the vehicle v_k falsifies its geolocation to simulate being on a cheaper pathway by making the OBU reports false information. Afterwards, it transmits the fake geolocation tuple $\langle P_{v_k}, L_{v_k}, T_{v_k} \rangle$ to the toll server via the RSU within its communication range. The RSU verifies the validity of the received vehicle geolocation referring to its own geolocation L_{RSU} such as

$$L_{RSU} \in [L_{v_k} - \mathcal{R}_{RSU}, L_{v_k} + \mathcal{R}_{RSU}], \tag{6}$$

where $\mathcal{R}_{RSU}$ represents the RSU communication range. If the condition holds, the RSU routes the geolocation tuple $\langle P_{v_k}, L_{v_k}, T_{v_k} \rangle$, else, it alerts the toll server about the attempted fraudulent action.

In the second scenario, the vehicle v_k driver turns off his own OBU to avoid transmitting its geolocation. To prevent such infringement and detect the fraudulent vehicle, a V2V communication based coordination process is executed. This mechanism uses the Advanced Driver Assistance Systems (ADAS) such as the cameras and radar to get precise information about the fraudulent vehicle. Upon the vehicle v_i receives a message from its neighbor v_j, it estimates the distance D_{ij}, which separates it from v_j through the signal strength (e.g., RSSI [14]). Meanwhile, the vehicle v_i uses its stereo camera and radar to monitor its entourage, thereby detecting the vehicles v_j and v_k. This information is then combined and processed to compute the distance D_{ik}. The latter distance allows the vehicle v_i to affirm the vehicle v_k fraudulent action if

$$D_{ik} < D_{ij}, \tag{7}$$

and no message has been received from v_k. Finally, the toll server identifies the suspected vehicle in order to apply the appropriate countermeasures.

In general, road pricing systems are introduced to manage road congestion and maintain rapid traffic flow in heavily used roads during peak hours. In fact, road pricing systems work better on roads and highways that are frequently visited and with long delays during congested periods. Without such congestion, authorities responsible for traffic management will not readily gain public acceptance of road pricing systems, and citizens will have little incentives to pay significant tolls. Despite the charging tolls, road pricing systems do not eliminate congestion, and some drivers would rather pay for moving on the best roads during the most convenient hours. Moreover, drivers are charged based on road pricing rates which vary for different roads and time periods depending on actual traffic conditions. Therefore, drivers that travel during non-pricing hours pay less or do not have to pay at all, which minimizes the risk of fraud in case of dishonest vehicles having their OBU switched off and without neighbors in the coverage area.

The SRP system keeps for the accused drivers evidences against them, including the geolocation and the time for which they omitted to pay. To prove the misbehavior of a given vehicle, a photograph of its license plate bound up with the time and geolocation, where it was spotted in is sent to the toll server through the accuser vehicles. After verification, the toll server invoices its owner by accumulating an extra fine, while a discount on their tolling bills is offered to the alerter drivers. Furthermore, although the license plate photographs are taken as evidences alerting fraudulent actions, a compromised vehicle could use this way to overwhelm innocent vehicles in order to thwart their drivers to pay more for their tolling bills. To prevent such kind of violation, we propose a $\langle t, n \rangle$ based threshold control system. A group $V = \{v_1, v_2, ..., v_n\}$ sharing the ability to cosign the evidences, where a sub-set of t vehicles of them can generate a valid signature.

With the aim to use standard cryptographic techniques, the proposed approach takes into account the inherent characteristics of road traffic. Indeed, before applying the fraudulent evidences signature scheme, we propose a group formation approach based on some relevant criteria, related to the vehicles mobility and behavior, in order to comply with actual road traffic scenarios. In fact, the vehicles that form the groups to cosign the evidences of fraud must share the same journey as long as possible. For instance, due to the dynamic nature of

vehicular networks, the vehicles of a same group must travel at approximately the same average speed to remain in communication range for a long time. Moreover, vehicular networks undergo frequent change of topology where the number of vehicles changes with time. Indeed, vehicles traveling on the road can change their trajectory at any time, which changes the number of vehicles at a significant place. For this reason, the proposed group formation approach selects adjacent vehicles of a same group in such a way that they must share the same route to perform the fraudulent evidences signature process.

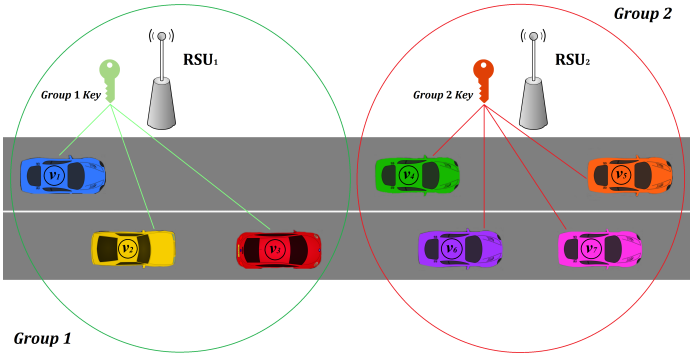

Fig. 4: Threshold control system group formation

As illustrated in Fig. 4, when several vehicles are in a same toll road, a coordinator RSU launches the process of groups formation. The coordinator RSU is the one within communication range of all the vehicles present on the toll road section where a malicious vehicle has been detected. For each group, a set of n honest vehicles are selected such, they remain as long as possible adjacent during the trip. For this purpose, the proposed approach takes in charge three important metrics in the group formation, namely, the vehicle itinerary, speed and reputation. After collecting such information, the coordinator RSU estimates for each pair of adjacent vehicles v_i and v_j the opportunity to be in the same group following the objective function $\mathcal{F}$ such as

$$\mathcal{F}(i,j) = \alpha \cdot I_{ij} + \beta \cdot S_{ij} + \gamma \cdot R_{ij}, \tag{8}$$

where α, β, and γ are coefficients to set regarding the metrics importance following the targeted application field, and

$$\alpha + \beta + \gamma = 1. \tag{9}$$

The vehicles v_i and v_j can belong to a same group, if and only if

$$\mathcal{F}(i,j) \geq \mathcal{R}, \tag{10}$$

where $\mathcal{R}$ denotes the degree of resemblance and represents how far two vehicles can remain together longer during their trip. Hence, it determines the optimal value for a natural group formation and gives a precise idea on the logic of belonging to the same group. The value of parameter $\mathcal{R}$ is set following the targeted application field and actual road traffic conditions. The metric $I_{ij} \in [0,1]$ represents the adjacency degree of the pair of vehicles v_i and v_j during the trip. In fact, as most of the itineraries are currently obtained through GPS navigation systems according to a given destination, the drivers are more likely to take the shortest routes. Therefore, the probability that vehicles v_i and v_j make the same journey will be high if they are heading towards the same destination. Hence, this metric has to be maximized and is quantified by the similarity rate of vehicles itineraries. The metric $S_{ij} \in [0,1]$ denotes the speed similarity of the pair of vehicles v_i and v_j. Indeed, if v_i and v_j travel at approximately the same average speed then there is a high probability that they will remain adjacent for a long time during their trip. In fact, two honest vehicles traveling at different speeds in different lanes cannot corroborate a dishonest driver, because vehicles that form the group must be within direct communication range to prevent any type of attacks during the fraudulent evidences signature process (e.g., replay attacks, fraud evidences falsification, etc.). If the vehicles travel at different speeds, intermediates are needed to transmit messages and perform the fraud evidences signature scheme, which increases the risk of such attacks. Therefore, the metric S_{ij} has also to be maximized and is computed such as

$$S_{ij} = \frac{S_i^2\Big(\operatorname{sgn}(S_j - S_i) + 1\Big) + S_j^2\Big(\operatorname{sgn}(S_i - S_j) + 1\Big)}{2S_iS_j}, \tag{11}$$

where S_i and S_j denote, respectively, the average vehicles v_i and v_j speeds. Finally, $R_{ij} \in [0,1]$ denotes whether the vehicles v_i and v_j reputation values are well-matched such as

$$R_{ij} = R_i \cdot R_j. \tag{12}$$

A reputation variable R_i represents the degree of trust, measured in percentage (%), that the system has about the vehicle v_i. We assume that the vehicle v_i reputation value R_i is measured by the number of times the vehicle v_i is accused to be malicious. This metric is handled by the toll server and updated following the vehicles behaviors, which is introduced in order to avoid dishonest vehicle in the group formation since we should not trust a vehicle that has already acted maliciously (e.g., by attempting to cheat on his tolls, by do not reporting the malicious vehicles it has detected, etc.) to join a group and corroborate fraudulent vehicles. In fact, the reputation values R_i and R_j determine how trustworthy the vehicles are regarding their past behaviors. Hence, vehicles v_i and v_j are more likely to collaborate and corroborate a dishonest vehicle if they have high reputation values. Hence, maximizing the metric R_{ij} amounts to maximize the variables R_i and R_j individually in order to favor the integration of vehicles with good reputation in the group.

Trust and reputation management in vehicular networks is a well-investigated subject in the literature, which we have not addressed precisely in this paper. However, there are several trust models that have been proposed in the literature to enforce honest information sharing and evaluate how trustworthy the communicating vehicles are. Moreover, there are various new approaches that address the detection of intelligent malicious behaviors, where dishonest vehicles are assumed

intelligent enough to adapt and vary their behavior over time in order to avoid being detected and excluded from the network [1], [7], [15].

D. Fraudulent evidences signature and verification

We design the threshold control system on the signcryption scheme proposed in [22]. Through a $\langle t, n\rangle$ threshold scheme, we consider a group $V = \{v_1, v_2, ..., v_n\}$ of legitimate vehicles, where n is the number of vehicles in the group V formed by the coordinator RSU. The parameter value n depends then on the number of adjacent vehicles that are selected following the objective function described in equation (8). As for the parameter t, there are several solutions that have been done about whether the value of t should be variable or fixed. The threshold t could be set as a variable parameter, which its value changes over the time, as what have been proposed in some existing solutions in the literature [30], [31], [32]. The value of the threshold t will be then negotiated at the time of group formation. Once formed, the group vehicles share a private key and cooperate to produce the evidences signature against any dishonest vehicle during the trip. Any $t-1$ or fewer vehicles cannot rebuild the private key or forge a valid signature. Even when an attacker that can compromise at most $t-1$ vehicles cannot discover any information about the private key. All the group V operations are handled by coordinator RSUs, which are responsible for partial key distribution, partial signature collection and verification, and group signature computation.

First, a coordinator RSU generates the group V private key $\widehat{K}_V \in [1, q-1]$, computes its corresponding public key K_V such as

$$K_V = \widehat{K}_V \cdot Q, \tag{13}$$

and publishes the public parameters p, q, $E_p(a, b)$, Q, K_V and K_S. Then, it randomly chooses a secret polynomial $\mathcal{G}$ of degree $t-1$ such as

$$\mathcal{G}(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1} \bmod q, \tag{14}$$

where

$$\mathcal{G}(0) = a_0 = \widehat{K}_V. \tag{15}$$

Finally, it computes the vehicle v_i private share $\widehat{K}_V^{(i)}$ such as

$$\widehat{K}_V^{(i)} = \mathcal{G}(i), \tag{16}$$

and publishes the corresponding public share $K_V^{(i)}$ such as

$$K_V^{(i)} = \widehat{K}_V^{(i)} \cdot Q. \tag{17}$$

Over a secure communication channel, the coordinator RSU sends for each vehicle $v_i \in V$ its private share $\widehat{K}_V^{(i)}$.

Suppose that a vehicle v_k passes over a given geolocation L_{v_k} at a given time T_{v_k} while disabling its OBU. A subset of t adjacent vehicles from V will then collaboratively produce the evidence $\mathcal{E}_k = \langle L_{v_k}, T_{v_k}\rangle$ signature. This evidence is a proof of the vehicle v_k infringement and has to be sent to the toll server. To do this, each vehicle $v_i \in V$ chooses a random number $c_i \in [1, q-1]$, and computes Y_i and Z_i such as

$$Y_i = c_i \cdot Q, \tag{18}$$

and

$$Z_i = c_i \cdot K_S. \tag{19}$$

The set of Y_i and Z_i are sent over a secure communication channel to a coordinator RSU within their range. Upon receiving, the coordinator RSU computes Z and r such as

$$Z = \sum_{i=1}^{t} Z_i, \tag{20}$$

and

$$r = \mathcal{E}_k \cdot x_Z \bmod p. \tag{21}$$

Afterwards, the coordinator RSU broadcasts r to the vehicles $v_i \in V$, where each one of them computes x_i and e_i such as

$$x_i = \prod_{j=1, j\neq i}^{t} \frac{-j}{(i-j)} \bmod q, \tag{22}$$

$$e_i = \widehat{K}_V^{(i)} \cdot x_i \bmod q, \tag{23}$$

and responds by its partial signature s_i such as

$$s_i = c_i - e_i \cdot r \bmod q. \tag{24}$$

Upon receiving at least t partial signatures, the coordinator RSU computes Y_i' such as

$$Y_i' = r \cdot x_i \cdot K_V^{(i)} + s_i \cdot Q. \tag{25}$$

If $Y_i = Y_i'$ for all the partial signatures, the coordinator RSU computes s such as

$$s = \sum_{i=1}^{t} s_i \bmod q. \tag{26}$$

Finally, $\sigma_E = \langle r, s, Y_1, Y_2, ..., Y_t\rangle$ is the group V signature, which is sent to the toll server. The latter can then verify the validity of the signature using the group V public key K_V. To do this, the toll server computes Y, Y' and Z' such as

$$Y = \sum_{i=1}^{t} Y_i, \tag{27}$$

$$Y' = r \cdot K_V + s \cdot Q, \tag{28}$$

and

$$Z' = \widehat{K}_S \cdot Y'. \tag{29}$$

If $Y = Y'$, then the signature is valid and the toll server decrypts $\mathcal{E}_k$ such as

$$\mathcal{E}_k = r \cdot x_{Z'}^{-1} \bmod p. \tag{30}$$

E. Tolling bill signature and verification

Algorithm 1 Tolling bill signature by the toll server

Inputs: $\{\langle L_i^l, T_i^l\rangle\}_{l=1}^{N}$, K_i
$\mathcal{C}_i \leftarrow 0$;
$\mathcal{B}_i \leftarrow \varnothing$;
for all $1 \leq l \leq N$ **do**
$\mathcal{C}_i \leftarrow \mathcal{C}_i + f(L_i^l, T_i^l)$;
$\mathcal{B}_i \leftarrow \mathcal{B}_i || \langle L_i^l, T_i^l\rangle || f(L_i^l, T_i^l)$;
end for
$\mathcal{B}_i \leftarrow \mathcal{B}_i || \mathcal{C}_i$;
Choose $c \in [1, q-1]$;
$Y_1 \leftarrow c \cdot Q$;
$Y_2 \leftarrow c \cdot K_i$;
$r \leftarrow \mathcal{B}_i \cdot x_{Y_2} \bmod p$;
$s \leftarrow c - \widehat{K}_S \cdot r \bmod q$;
$\sigma_{\mathcal{B}_i} \leftarrow \langle r, s, Y_1\rangle$;
return $\sigma_{\mathcal{B}_i}$;

At the pricing period end, the toll server produces the final tolling bill and sends it to the registered drivers. The tolling bill is signed by the toll server to guarantee its integrity as well as its authenticity. For each tuple $\langle L_i^l, T_i^l\rangle$, the toll server computes the fee $f(L_i^l, T_i^l)$ of the driver d_i. The partial fees are accumulated to figure-out the driver d_i tolling bill, denoted by $\mathcal{B}_i$, with the total amount to pay, denoted by $\mathcal{C}_i$. The structure of $\mathcal{B}_i$ is as follows

$$\mathcal{B}_i = \langle L_i^1, T_i^1, f(L_i^1, T_i^1)\rangle || ... || \langle L_i^N, T_i^N, f(L_i^N, T_i^N)\rangle || \mathcal{C}_i, \tag{31}$$

where N represents the number of times the driver d_i enters toll roads. The final step consists of encrypting the tolling bill using the vehicle v_i public key and then signing it using the toll server private key. To do this, the toll server uses a secure elliptic curve $E_p(a, b)$ over a finite field F_p and a base point Q of a prime order of q. These parameters were publicly agreed on with the driver d_i during the initialization phase. The toll server chooses randomly $c \in [1, q-1]$, and computes Y_1 and Y_2 such as

$$Y_1 = c \cdot Q, \tag{32}$$

and

$$Y_2 = c \cdot K_i. \tag{33}$$

Afterwards, it computes r and s such as

$$r = \mathcal{B}_i \cdot x_{Y_2} \bmod p, \tag{34}$$

and

$$s = c - \widehat{K}_S \cdot r \bmod q. \tag{35}$$

Finally, it outputs the signature $\sigma_{\mathcal{B}_i} = \langle r, s, Y_1\rangle$ incorporating the tolling bill $\mathcal{B}_i$ hidden in r. In case of a reported fraudulent action, an extra fine will be added to the tolling bill of the dishonest drivers. The process of tolling bill elaboration is summarized in Algorithm 1.

At the pricing period end, each driver receives his tolling bill. Before payment, the OBU authenticates the tolling bill signature using the toll server public key and recovers the path tolling cost. The driver proceeds to the payment if the signature is valid. To do this, the vehicle v_i checks the following equality

$$r \cdot K_S + s \cdot Q = \widehat{K}_i \cdot Y_1'. \tag{36}$$

If it holds, the tolling bill $\mathcal{B}_i$ is rebuilt such as

$$\mathcal{B}_i = r \cdot x_{Y_2'}^{-1} \bmod p. \tag{37}$$

The process of tolling bill signature verification is summarized in Algorithm 2.

Algorithm 2 Tolling bill verification by the vehicle v_i

Inputs: $\sigma_{\mathcal{B}_i}$, K_S
$Y_1' \leftarrow r \cdot K_S + s \cdot Q$;
$Y_2' \leftarrow \widehat{K}_i \cdot Y_1'$;
if $(Y_1 = Y_1')$ **then**
$\mathcal{B}_i \leftarrow r \cdot x_{Y_2'}^{-1} \bmod p$;
return $\mathcal{B}_i$;
else
return signature invalid;
end if

F. Tolling bill format

To comply with the smart city paradigm that aims to improve and simplify the services offered to citizens, the SRP system has to invoice the users in digital format by adopting electronic tolling bills as a simple and practical service. We propose a approach for the tolling bill. The latter is organized in three parts including information related to the tolling bill, information about its owner, and information related to the toll server. Fig. 5 illustrates a tolling bill, which comprises in addition to the bill details, the specification of the digital signature algorithm used by the toll server in the signature generation. For the drivers who were suspected dishonest, information on the toll evasion violation appear in their final tolling bill with the digital evidence generated by the group of signers, as depicted in Fig. 6. There are several aspects of the billing phase that must be taken into consideration to produce the final tolling bill for a given driver. However, the proposed approach does not tackle the billing details given the large scope of the addressed thematic in this paper. Therefore, our proposed approach does not exclude other types of applications.

V. Security Analysis

In this section, we discuss how the proposed approach resists against attacks and satisfies the security properties in the context of SRP fraud detection.

A. Impersonation attack

At the entrance of a toll road, a compromised vehicle can eavesdrop the network. It then tries to obtain information about

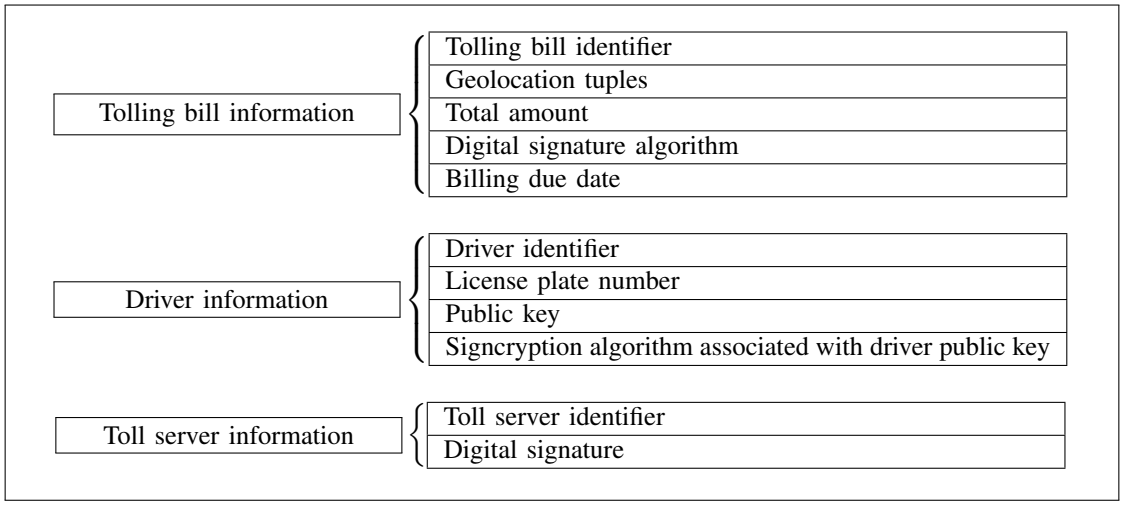

Fig. 5: Normal tolling bill

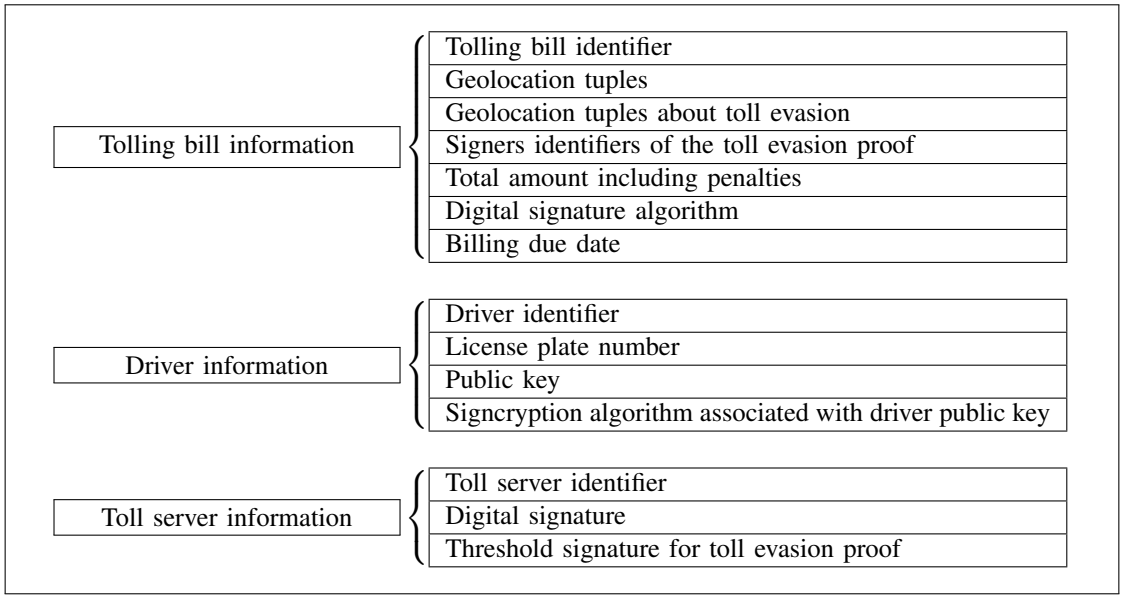

Fig. 6: Tolling bill in case of fraudulent action(s)

legitimate vehicles identities to eventually impersonate them later. To prevent such fraudulent action, the proposed approach dynamically assigns for each vehicle a pseudonym based on a shared secret between the RSU and vehicle. As the pseudonym generation process is based on Elliptic Curve Diffie-Hellman exchange, any third party that intercepts the exchanged public keys K_{RSU} and K_i, would not be able to find out the shared secret ℓ_i and recover the vehicle pseudonym. Moreover, the pseudonyms are generated based on timestamps. This prevents a driver from reusing a past pseudonym to reduce his tolling bill amount. In fact, even if he tries to reuse a valid pseudonym in another toll session, the fraudulent driver will be detected as each pseudonym is uniquely bound to the real driver identity, and all the RSUs along the toll road are aware of this correspondence.

B. Privacy

Privacy is of the utmost importance in vehicular networks as the vehicles have communication abilities. The proposed approach ensures the two privacy aspects, namely, the anonymity and the unlinkability. Anonymity holds when the driver identity does not need to be disclosed. To prevent such leaking, whenever a vehicle generates its geolocation tuple, only a pseudonym is specified in the message sent to the RSU. Moreover, the proposed approach ensures conditional unlinkability as the pseudonym will be different for the same vehicle even if it takes the same road another time. In fact, the pseudonyms are determined by the time at which a vehicle enters a toll road and the nearest RSU identity at this time. Hence, for any different execution of the protocol, an attacker eavesdropping the communications has no way to link the pseudonyms to the actual driver identity and learn the geolocations he traveled.

C. Collusion resistance

During driving, a compromised vehicle may try to rise the tolling bill of a given driver by taking a photograph of his license plate and transmitting it to the toll server. This photo proves the driver guilty in fraud and will be used as an evidence to justify the extra fine. To prevent such misbehavior, the proposed approach shares the evidences signature ability among a group of several vehicles, which collaborate to cosign the toll evasion proofs that will appear on the final tolling bill. It is thus unlikely that t or more vehicles from the group conspire to generate a valid signature against a same driver at a given time. Hence, counteracting such collusion attacks depends on the threshold parameter t following the targeted application field. In fact, in presence of a large number of dishonest vehicles, the threshold value t has to be set high enough to prevent any collusion. On the other hand, if there are only few dishonest vehicles, the value of parameter t can be decreased to gain efficiency while ensuring security.

D. Accountability

Accountability means that the fraudulent drivers should be identified and evidences against them should be recorded. If a dishonest driver tries to fraud, honest drivers provide to the toll server a sufficient evidence to identify that driver. Moreover, even if he does not participate in the tolling process by deliberately disabling his OBU system, he will still be charged by the toll server based on the geolocation data provided by the other vehicles. Although it encroaches slightly on the fraudulent drivers privacy, this punishment policy aims to discourage such infringements and improve the efficiency of the SRP system.

E. Confidentiality and unforgeability

To guarantee that only the vehicle driver be able to get access to his tolling bill, the proposed approach relies on a signcryption scheme, which can simultaneously fulfill both the functions of digital signature and public key encryption. It is thus suitable in such cases, where both confidentiality and authenticity are required. In fact, only a given vehicle v_i, which holds the private key $\widehat{K}_i$ is able to decrypt the tolling bill $\mathcal{B}_i$. Moreover, in case of fraud detection of the driver, an attacker cannot forge the evidences signature to deceive him with an increased toll amount. This misbehavior can be checked from redundant information of the evidence due to the ability of signature that has been shared among several vehicles.

VI. Performances evaluation

In this section, we evaluate the efficiency of the proposed approach. We have conducted intensive simulations with a comparison to the reviewed approaches presented in Section II. In what follows, we present the simulation environment, the performance metrics, and finally, we discuss the obtained results.

A. Simulation environment and parameters

The simulations are developed using the programming language Java. We have generated the mobility scenarios using the vehicular mobility generator SUMO (Simulation of Urban Mobility) [27]. We have combined SUMO with OpenStreetMap [28] by simulating a traffic in an area of 1.5km^2 in the Bejaia city (Algeria) as depicted in Fig. 7. The geolocation data derived from OpenStreetMap were edited by JOSM (Java OpenStreetMap) [29]. The resulting mobility traces are then fed into the developed simulator as the vehicles geolocations. The simulation duration is of 1000s and the performance measurements are averaged based on the results obtained for 50 iterations. Each vehicle starts transmitting its geolocation upon entering the toll road after 10s. We consider a geolocation tuple of 32 byte, which contains latitude, longitude, date and time. The geolocation tuples are sent to the RSUs within the vehicle communication range, deployed at fixed positions along the toll road. The simulations were conducted in the presence of up to 30% of compromised vehicles.

As regards the reviewed approaches, the performance measurements are performed in the same simulation environment as for the proposed solution. In fact, each vehicle sends a geolocation tuple of 32 byte to the RSU within its communication range deployed along the toll road. Moreover, we consider some parameters values following the cryptographic techniques used in each protocol. For instance, in [20] and [18], we consider commitments of 130 byte used to prevent the disclosure of drivers geolocation, and a NIZK proof of 5455 byte to prove the validity of the committed values. Besides, blind IBE keys of 494 byte are used in [18] to prevent drivers collusion and strengthen the random spot checks. The different public and private keys, used by OBUs and RSUs in the various protocols, are of 256 byte which correspond to high security level. To prevent toll evasion violations, the spot checks cameras deployed along the toll roads take a photograph of each vehicle passing through. To perform the simulations, we consider license plate photos of 20 kbyte sent to the toll server. The simulation parameters details of the various protocols are summarized in Table III.

TABLE III: Size of the parameters in the reviewed protocols

Parameter	**Size (byte)**
Identifiers	2
Geolocation tuples	32
Public and private keys	256
Commitments	130
IBE ciphertexts	366
NIZK proofs	5455
Blind IBE keys	494
Hash of geolocation tuples	64
Public key certificates	256
License plate photos	21216

Before we evaluate the performances of the proposed approach, we were interested to study the impact of the metrics α and β on the objective function $\mathcal{F}$ in threshold signature group formation. We have conducted preliminary simulations with

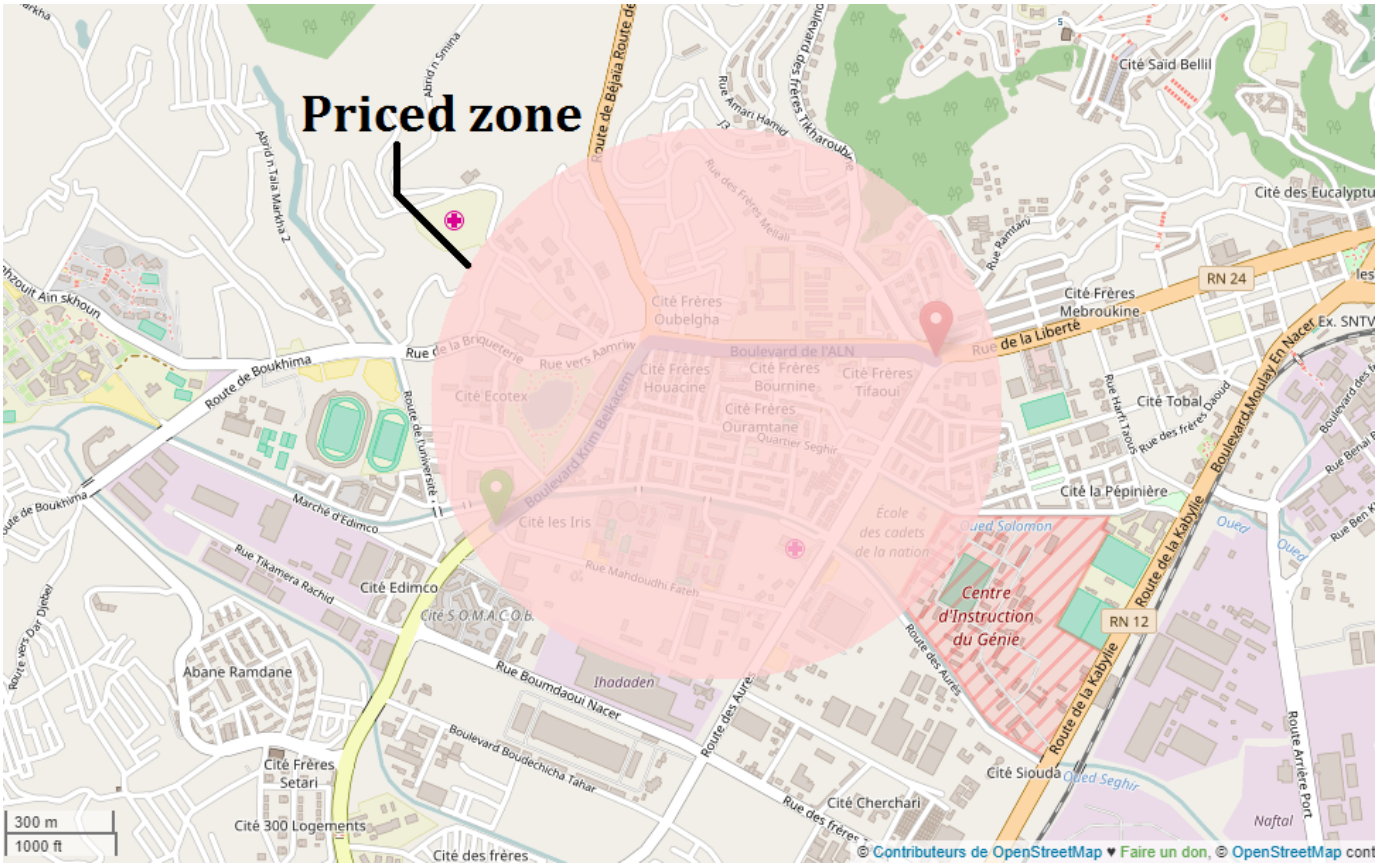

Fig. 7: Area of the vehicular mobility simulation

compromised vehicles presence to determine the best values of α and β, which maximize the function $\mathcal{F}$. We have considered two simulation scenarios according to the application sensitivity, namely, moderately sensitive applications with $\gamma = 0.3$, and highly sensitive applications with $\gamma = 0.5$. The obtained results for both scenarios are illustrated in Fig. 8 and 9, respectively, in which the maximum value of $\mathcal{F}$ is highlighted. Regarding the results, the degree of resemblance $\mathcal{R}$ is reached with $\alpha = 0.6$ and $\beta = 0.1$ for the first scenario, and with $\alpha = 0.4$ and $\beta = 0.1$ for the second one. For the proposed system, we perform the rest of simulations considering the second scenario, which corresponds to the resemblance degree $\mathcal{R} = 0.449$.

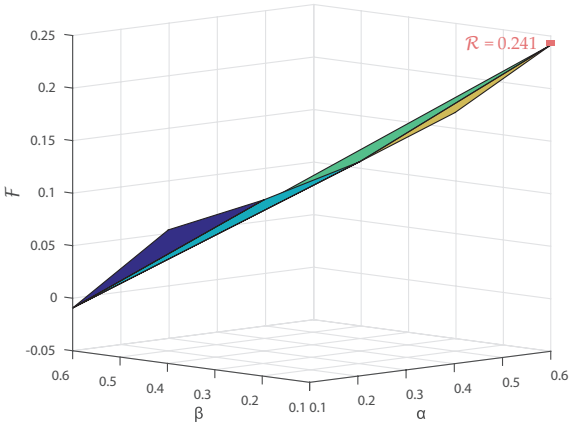

Fig. 8: Objective function $\mathcal{F}$ over α and β variation with $\gamma = 0.3$

B. Performance metrics

We evaluate two important performance metrics, namely, the storage and communication loads. Through the first metric, we evaluate how well the proposed approach handles the resource-constrained OBUs. As we can expect to have very scalable vehicular networks with hundreds of vehicles, managing huge amount of data, the storage load is an important metric to take in charge. The storage is estimated by the total amount of bytes stored in the OBUs and RSUs. Through the second metric, we evaluate how well the proposed approach optimizes the vehicular message exchanging. Reducing the communication load allows to cope with the inherent characteristics of such network such as the high dynamic topology and short connection duration, as well as the environmental impact on the generated radio signals due to the road obstacles (e.g. buildings, trees, billboards, etc.), which prevent their correct propagation. The communication load is estimated by the total amount of bytes exchanged by the OBUs and RSUs.

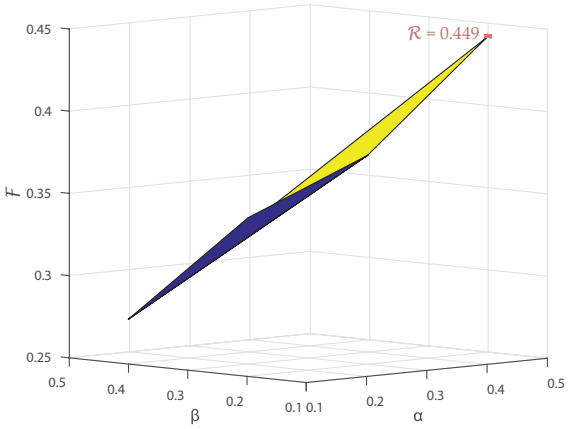

Fig. 9: Objective function $\mathcal{F}$ over α and β variation with $\gamma = 0.5$

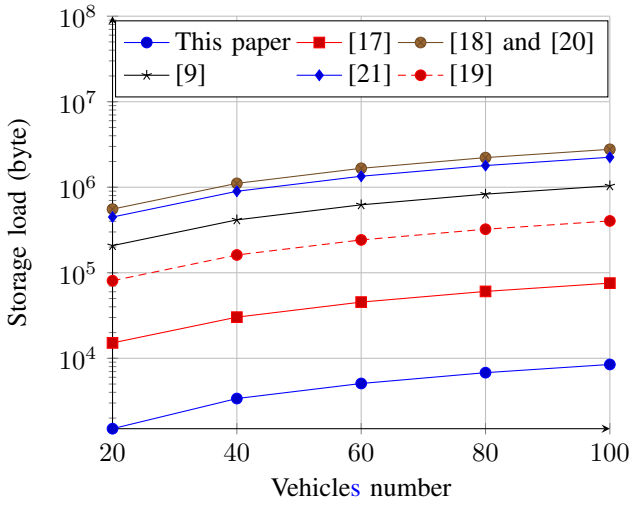

Fig. 10: Storage load in function of the vehicles number

C. Network size impact

Fig. 10 illustrates the storage load in function of the vehicles number in the network. The proposed approach shows better results compared to the other protocols. Indeed, the vehicle geolocation does not need to be stored into the OBU, and is directly transmitted to the toll server when the vehicle enters a toll road. The main parameters that the OBUs and RSUs need to store consist in the identifier of 2 byte, public and private keys of 20 byte, which results in a slight increase of storage load unlike the other protocols. In fact, the proposed approach relies on ECC to sign the fraud evidences, which minimizes the storage load as the OBUs store keys of small sizes while ensuring equivalent security level as the other protocols that rely on expensive public key cryptosystems (e.g., RSA with keys of 256 byte for a high security level). Hence, the proposed solution offers improved security with reduced computational requirements compared to the other protocols. For instance, the protocol [18] presents a high increase of storage load due to the cryptographic proofs used to show the OBU honesty. In fact, as the geolocation tuples are stored into the vehicle to avoid vehicles whereabouts disclosure, the OBU stores a NIZK (Non-Interactive Zero Knowledge) proof of 5455 byte for each traveled road segment. In the protocol [9], the OBUs need to store several public keys to communicate with the various entities of the system (i.e., the checkpoints, the certification authorities, the service provider, the punishment authority, etc.), which results in a high increase of the storage load. Moreover, the certification authority installed in each vehicle generates credentials which consists of an asymmetric key pair and a public key certificate of 256 byte containing some extensions (e.g., the encryption of the vehicle identifier, its pollutant emission category, etc.) each time the vehicle enters a low emission zone in order to avoid link-ability between its trips.

Fig. 11 illustrates the communication load in function of the vehicle number. The obtained results show that the proposed approach offers better performances compared to the other protocols with a minor increase as the vehicles number rises. In fact, in the proposed solution, the OBU only sends its geolocation tuple of 32 byte to the neighboring RSU deployed along the toll road, and a partial signature of 20 byte in the case where the vehicle has join a group to report fraud actions. This results in a slight increase of the communication load in comparison to the other protocols. We also note that the protocols [18] and [9] present the same increase of the communication load. Indeed, in addition to the payment message of 5955 byte per segment, the protocol [18] penalizes all the vehicles by performing an auditing protocol after each pricing period. Hence, the OBU of each vehicle sends a blind IBE key of 494 byte for several segments that correspond to each camera the vehicle has been seen on. By opposition, in the protocol [9] even though, the cameras take a photograph evidence of compromised vehicles only, the OBUs and RSUs exchange tuples including the message m, its signature σ_m, and the public key certificate at each entrance, change or departure of a low emission zone. The message m can be an information of entrance, an authentication response, a photo warning, a proof of entrance, change or departure, etc. This implies a high increase of the communication load. The obtained results show the effectiveness of the proposed approach for SRP systems, even in emergent situations such as traffic congestion during peak hours.

D. Communication range impact

Fig. 12 illustrates the storage load in function of the communication range. Regarding the obtained results, the proposed approach shows better performances compared to the other protocols. In the proposed approach, we note a slight increase of the storage load for a communication range of less than 150m due to the threshold signature group formation. In fact, as the communication range increases, the neighboring vehicles number susceptible to form the group increases as well, which adds up an overhead to the basic storage load. Although the communication range has no impact on the storage load of the other protocols, the obtained results remain high compared to the proposed approach.

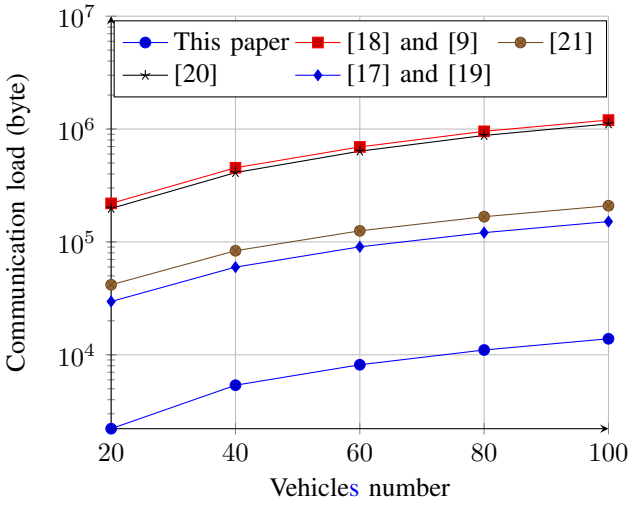

Fig. 11: Communication load in function of the vehicles number

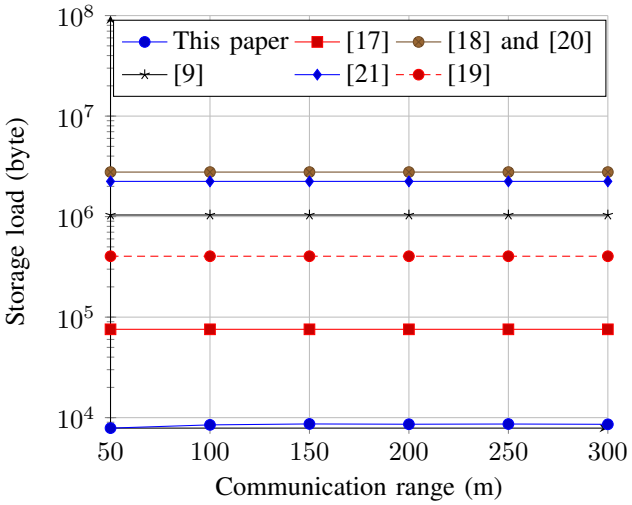

Fig. 12: Storage load in function of the communication range

Fig. 13 illustrates the communication load in function of the communication range. The proposed approach demonstrates better results compared to the other protocols. As mentioned earlier, when the communication range increases, the vehicles number involved in the threshold signature group rises too leading to a slight increase of the communication load before the range reaches 150m. However, as the latter increases, the geolocation tuples retransmission to RSUs becomes unnecessary, and hence the communication load decreases. We also note a slight gap between the protocols [18], [9] and [20]. Indeed, in the protocol [18], the OBU sends a payment message of 5955 byte for each road segment, which results in a considerable communication load, whereas the protocol [9] requires that the OBU communicates with a RSU each time the vehicle enters, changes or leaves the toll road. Moreover, when the authentication protocol fails, the RSU sends to the compromised OBU a warning message including the license plate photograph of 20 kbyte as an evidence of its infringement. On the other hand, in the protocol [20], the OBU sends at the end of each tax period a payment message m of 5653 byte and its signature σ_m of 128 byte. The message m consists of all the payment tuples (h, c_p, π), where h is a 64 byte hash of the geolocation information, c_p the price commitment of 130 byte, and π a NIZK proof of 5455 byte. Hence, the communication load remains high even with greater communication range.

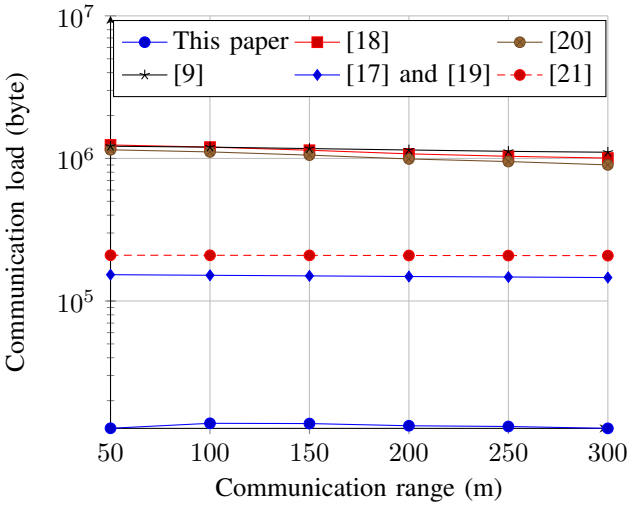

Fig. 13: Communication load in function of the communication range

E. Detection precision

We have evaluated the performances of the proposed approach in the detection of compromised vehicles that try to deceive the toll server by disabling their OBU. In this context, we have measured the detection rate in function of both network size and communication range. The detection rate denotes the ratio of the detected attacks to the total attack number. The simulations were conducted in the presence of various percentages of compromised vehicles. Fig. 14 illustrates the detection rate in function of the vehicles number in the network. The

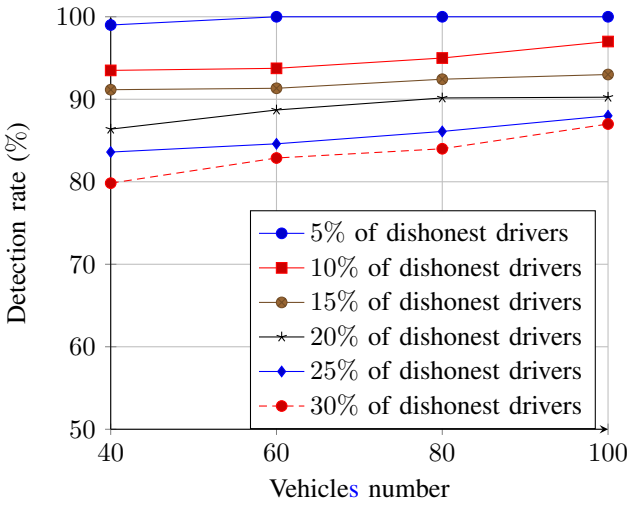

Fig. 14: Detection rate in function of the vehicles number

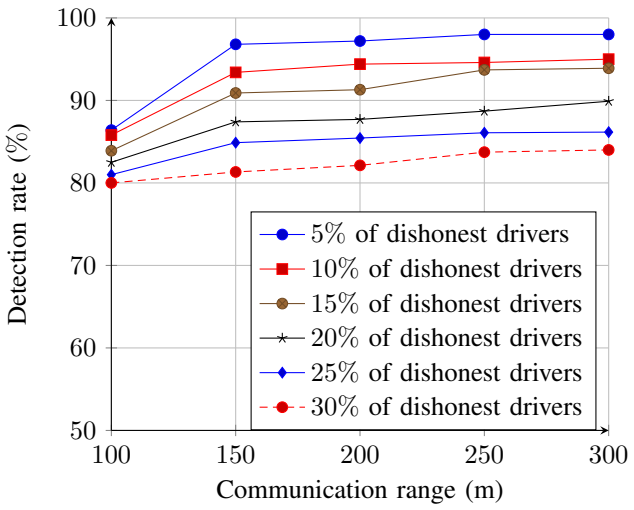

Fig. 15: Detection rate in function of the communication range

obtained results show that whatever the vehicles number on the road, the detection rate is greater than 80% even in the presence of 30% of compromised vehicles, which stands for an acceptable rate. Fig. 15 illustrates the detection rate in function of the communication range. Regarding the obtained results, we note a detection rate of 80% for a short communication range of 100m, which is acceptable. Moreover, the detection rate increases as the communication range becomes greater, which is quite understandable, in the fact that it allows the formation of high size groups. Indeed, a great communication range implies more V2V communications, hence the threshold signature group formation become increasingly possible. Compromised vehicles can be thus reported to the toll server.

VII. Conclusion

With the increasing vehicles number on the roads in most big cities, a smart traffic management solution has become a must necessity for the success of city management and the improvement of citizens quality of life. Recently, SRP has emerged as a promising solution to road congestion and air pollution. In fact, charging drivers for bringing their vehicles into congested areas will incite them either to avoid unnecessary journeys or to vary their times of travel, thereby reducing traffic jam and gas emissions. Although SRP systems seem to promise clear benefits, there are significant potential infringements such as toll evasion violations. In this paper, we have proposed a novel security approach for SRP systems, which detects such misbehavior. The main goal of this work is to spot fraudulent drivers, who cheat on their geolocations in order to save illegally money. The proposed approach relies on V2V communications and obstacle detection systems embedded in most new generation cars. It combines cryptographic primitives to protect drivers geolocation privacy and strengthen the guarantee of their honesty. In order to evaluate the efficiency of the proposed approach, we have performed intensive simulations and compared it to the concurrent approaches. The obtained results indicate better performances of the proposed approach in terms of storage and communication overheads. In fact, we observe that our proposed solution is 97% more performant in terms of storage load, and 95% more in terms of communication load compared to the other protocols. We have also evaluated the efficiency of the proposed approach in the detection of compromised vehicles and obtained promising results.

Acknowledgment

This work was carried out in the framework of the research activities in the laboratory LIMED, which is affiliated to the Faculty of Exact Sciences of the University of Bejaia.

References

[1] C-A. Kerrache, A. Lakas, N. Lagraa and E. Barka, *UAV-assisted technique for the detection of malicious and selfish nodes in VANETs*, Vehicular Communications 11, pp. 1–11, 2018.

[2] C. Bila, F. Sivrikaya, M-A. Khan and S. Albayrak, *Vehicles of the Future: A Survey of Research on Safety Issues*, IEEE Transactions on Intelligent Transportation Systems 18(5), pp. 1046–1065, 2017.

[3] A. Laouiti, A. Qayyum and M-N-M. Saad, *Vehicular Ad-Hoc Networks for Smart Cities*, In Proceedings of the Second International Workshop of Advances in Intelligent Systems and Computing, Vol. 548, Springer, 2017.

[4] F. Qin, R. Sun, W-Y. Ochieng, S. Feng, K. Han and Y. Wanga, *Integrated GNSS/DR/Road Segment Information System for Variable Road User Charging*, Transportation Research Part C: Emerging Technologies 82, pp. 261–272, 2017.

[5] A. Marefat, R-M. Noor, N-B. Anuar and N. Hussin, *The Feasibility of Employing IEEE 802.11p in Electronic-Based Congestion Pricing Zone: A Comparative Study with RFID*, Malaysian Journal of Computer Science 29(4), pp. 247–261, 2017.

[6] R. Harkanson and Y. Kim, *Applications of Elliptic Curve Cryptography: A light introduction to elliptic curves and a survey of their applications*, In Proceedings of the 12th Annual Conference on Cyber and Information Security Research, 2017.

[7] W. Li and H. Song, *ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks*, IEEE Transactions on Intelligent Transportation Systems 17(4), pp. 960–969, 2016.

[8] M. Soyturk, K-N. Muhammad, M-N. Avcil and J. Matthews, *From Vehicular Networks to Vehicular Clouds in Smart Cities, Smart Cities and Homes: Key Enabling Technologies*, Book, ISBN: 978-0-12-803454-5, 322(10), pp. 149–171, 2016.

[9] R. Jardi-Cedo, M. Mut-Puigserver, J. Castella-Roca, M. Magdalena and A. Viejo, *Privacy-preserving Electronic Road Pricing System for Multifare Low Emission Zones*, In Proceedings of the 9th International Conference on Security of Information and Networks, pp. 158–165, 2016.

[10] M. Alsabah and I. Goldberg, *Performance and Security Improvements for Tor – A Survey*, ACM Computing Surveys 49(2), Article No. 32, 2016.

[11] A. Dua, N. Kumar, M. Singh, M-S. Obaidat and K-F. Hsiao, *Secure Message Communication Among Vehicles Using Elliptic Curve Cryptography in Smart Cities*, In Proceedings of the International Conference on Computer, Information and Telecommunication Systems, pp. 1–6, 2016.

[12] B. Mukhopadhyay, S. Sarangi and S. Kar, *Performance Evaluation of Localization Techniques in Wireless Sensor Networks Using RSSI and LQI*, In Proceedings of the National Conference on Communications, pp. 1–6, 2016.

[13] S. Djahel, R. Doolan and G-M. Muntean, *A Communications-oriented Perspective on Traffic Management Systems for Smart Cities: Challenges and Innovative Approaches*, IEEE Communications Surveys and Tutorials 17(1), pp. 125–151, 2015.

[14] R-S. Yokoyama, B-Y. Kimura, L-A. Villas and E-D. Moreira, *Measuring Distances with RSSI from Vehicular Short-Range Communications*, International Conference on Computer and Information Technology, Ubiquitous Computing and Communications, Dependable, Autonomic and Secure Computing, Pervasive Intelligence and Computing, pp. 100–107, 2015.

[15] S-S. Tangade and S-S. Manvi, *A Survey on Attacks, Security and Trust Management Solutions in VANETs*, In Proceedings of the 4th International Conference on Computing, Communications and Networking Technologies, pp. 1–6, 2013.

[16] X. Chen, D. Fonkwe and J. Pang, *Post-hoc User Traceability Analysis in Electronic Toll Pricing Systems*, Data Privacy Management and Autonomous Spontaneous Security, pp. 29–42, 2013.
[17] X. Chen, G. Lenzin, S. Mauw and J. Pang, *A Group Signature Based Electronic Toll Pricing System*, In Proceedings of the 7th International Conference on Availability, Reliability and Security, pp. 85–93, 2012.
[18] S. Meiklejohn, K. Mowery, S. Checkoway and H. Shacham, *The Phantom Tollbooth: Privacy-Preserving Electronic Toll Collection in the Presence of Driver Collusion*, In Proceedings of the 20th USENIX Security Symposium, pp. 32–47, 2011.
[19] C. Troncoso, G. Danezis, E. Kosta, J. Balasch and B. Preneel, *PriPAYD: Privacy-Friendly Pay-As-You-Drive Insurance*, IEEE Transactions on Dependable and Secure Computing 8(5), pp. 742–755, 2011.
[20] J. Balasch, A. Rial, C. Troncoso and C. Geuens, *PrETP: Privacy-Preserving Electronic Toll Pricing*, In Proceedings of the 19th USENIX Security Symposium, pp. 63–78, 2010.
[21] R-A. Popa, H. Balakrishnan and A-J. Blumberg, *VPriv: Protecting Privacy in Location-Based Vehicular Services*, In Proceedings of the 18th USENIX Security Symposium, pp. 335–350, 2009.
[22] P. Changgen and L. Xiang, *Threshold Signcryption Scheme based on Elliptic Curve Cryptosystem and Verifiable Secret Sharing*, In Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1182–1185, 2005.
[23] D. Boneh and M. Franklin, *Identity-Based Encryption from the Weil Pairing*, Advances in Cryptology 2139, pp. 213–229, 2001.
[24] B. Pfitzmann, *Digital Signature Schemes*, Lecture Notes in Computer Science, Springer, 1996.
[25] D. Chaum and E. Van-Heyst, *Group signatures*, Advances in Cryptology, Lecture Notes in Computer Science, Vol. 547, pp. 257–265, Springer, 1991.
[26] A. Shamir, *How to Share a Secret*, Communications of the ACM 22(11), pp. 612–613, 1979.
[27] Simulation of Urban Mobility (SUMO), http://sumo.sourceforge.net, available online 27 July 2017.
[28] OpenStreetMap, http://www.openstreetmap.org, available online 27 July 2017.
[29] Java OpenStreetMap Editor, https://josm.openstreetmap.de, available online 27 July 2017.
[30] L. Harn and C-F. Hsu, *Dynamic threshold secret reconstruction and its application to the threshold cryptography*, Information Processing Letters, Volume 115, pp. 851–857, 2015.
[31] K. Hamouid and K. Adi, *Secure and robust threshold key management (SRKM) scheme for ad hoc networks*, Security and Communication Networks, Volume 3, Issue 6, pp. 517–534, 2010.
[32] C. Delerablee and D. Pointcheval, *Dynamic Threshold Public-Key Encryption*, Advances in Cryptology - Proceedings of CRYPTO, pp. 317–334, 2008.

Siham Bouchelaghem received the master's degree in Computer Science from the University of Bejaia, Algeria, in 2016. She graduated as the valedictorian of her class during both License and Master cycle. Currently, she is a PhD student in the Computer Science Department in the University of Bejaia, after winning the first place in the PhD entrance examination. She is also member of "Networking for Healthcare Applications" in the laboratory LIMED (Laboratoire d'Informatique MEDical). Her research interests include security and privacy in Smart Cities, Smart Traffic Management Systems, and Vehicular Ad hoc Networks.

Mawloud Omar is assistant professor in the university of Bejaia (Algeria), where he is member of the laboratory LIMED (Laboratoire d'Informatique MEDical) in the "Networking for Healthcare Applications" group. He got his PhD and Magister degrees in computer science from the university of Bejaia in 2011 and 2007, respectively. He got his engineer diploma in computer science from the university of Chlef (Algeria) in 2004. He was leader of the computer science department in the university of Bejaia from March 2012 to December 2015. His research activities revolve around security in computer science and network reliability, in particular the security problems of hardware, software, systems and networks. He is looking to the challenging issues related to the mobile networks, wireless sensor networks, wireless body area networks, social networks, vehicular networks, smart cities, quantum networks, the Internet of things and Big Data.