DYNA
ISSN: 0012-7353
ISSN: 2346-2183
Universidad Nacional de Colombia

Pseudonym change strategy based on the reputation of the neighbouring vehicles in VANETs

Santos-Jaimes, Luz Marina; Moreira, Edson dos Santos
Pseudonym change strategy based on the reputation of the neighbouring vehicles in VANETs
DYNA, vol. 86, no. 211, 2019
Universidad Nacional de Colombia
Available in: http://www.redalyc.org/articulo.oa?id=49663345018
DOI: 10.15446/dyna.v86n211.75602

Artículos

Pseudonym change strategy based on the reputation of the neighbouring vehicles in VANETs

Estrategia de cambio de seudónimo basada en la reputación de los vehículos vecinos en VANETs

Luz Marina Santos-Jaimes [a] lsantos@unipamplona.edu.co
Universidad de Pamplona, Colombia
Edson dos Santos Moreira [b] edson@icmc.usp.br
Universidade de São Paulo, Brazil

DYNA, vol. 86, no. 211, 2019

Universidad Nacional de Colombia

Received: 16 October 2018
Revised document received: 16 September 2019
Accepted: 18 October 2019

DOI: 10.15446/dyna.v86n211.75602

Abstract: Pseudonym change schemes have been studied in VANETs to guarantee the property of untraceability of the vehicles. This paper proposes a new condition based on the assumption that if there are no malicious vehicles around when a synchronous change triggers, there is no risk of tracking, and the pseudonym change defers until a time threshold. Thus, our proposal based on a synchronous strategy to increase the anonymity set, adds to the change condition, the checking of the reputation status of the neighbouring vehicles. The reputation status is the result of discretizing the reputation score of the vehicles and it is part of the periodically broadcasted beacon messages. The proposal was evaluated through experiments using a simulated scenario of a real map. The results showed an optimization in the use of pseudonyms maintaining similar anonymity levels with other schemes.

Keywords: vehicular network, privacy, pseudonym change, reputation.

Resumen: Esquemas de cambio de seudónimos han sido estudiados en VANETs para garantizar la propiedad de no rastreo de los vehículos. Este artículo propone una nueva condición basada sobre la suposición de que sí no hay vehículos maliciosos alrededor cuando un cambio síncrono activa, no hay riesgo de rastreo, y el cambio de pseudónimo es extendido hasta un máximo tiempo de espera. Así, nuestra propuesta basada en una estrategia síncrona, adiciona a la condición de cambio, el chequeo del estatus de reputación de los vehículos vecinos. El estado de reputación es el resultado de discretizar la puntuación de reputación de los vehículos y es parte de los mensajes de seguridad difundidos periódicamente. La propuesta fue evaluada mediante experimentos usando un escenario simulado de un mapa real. Los resultados mostraron una optimización en el uso de pseudónimos manteniendo niveles de anonimidad similar con otros esquemas.

Palabras clave: red vehicular, privacidad, cambio de pseudónimo, reputación.

1. Introduction

As the Vehicular Ad hoc NETworks (VANETs) are becoming a key component of Intelligent Transport System (ITS), the deployment of safety and non-safety applications will be compromised unless there are proper security and privacy mechanisms. In this context, the IEEE 1609.2 [1] and ETSI TS ITS 102-941 [2] security standards recommend the use of digital signature algorithms to ensure authenticity, integrity and non-repudiation in the exchange of sensitive messages. However, this does not guarantee the privacy of the vehicles, inside intruders with

legitimate credentials or global adversary could be able to trace vehicles by eavesdropping on vehicular communications. Privacy in VANETs is achieved through two properties - unlinkability and untraceability; the first means that it should be impossible for an unauthorised entity to link the identity of the vehicle with that of its driver; and the second one states that it should not be possible to trace the movements of the vehicle [3]. The vehicles will have pseudonyms issued by a Certificate Authority (CA) to provide both security and privacy, instead of only one long-term certificate that just guarantee the security [4]. Pseudonyms are short-term public key certificates that do not contain information that can reveal the identity of the driver. Moreover, a pseudonym changing strategy must be adopted for mitigating the risk of tracking to the vehicles, since messages signed under the same pseudonym could be linked to each other.

The authors in [5] presented a centralised approach called Anonymous Reputation Scheme (ARS) for trust management in VANETs. This involved adopting a Public Key Infrastructure (PKI) scheme, in which the vehicles will store the public key of the CA to validate the pseudonyms, without having to access the infrastructure. In addition, it involved implementing a Reputation Server, which registered the reputation score of the vehicles. In this paper, we include the activity of pseudonym changing in the vehicle by adding the checking of the reputation status of the neighbouring vehicles to the conditions of the synchronous strategy in [6]. The new condition bases on the assumption that if there are no malicious vehicles around when a change triggers, there is no risk of tracking, and the pseudonym change defers until a time threshold. The reputation status is the result of discretizing the reputation score of the vehicles and it is part of the periodically broadcasted beacon messages. Problems related to strategies of pseudonym change in the literature refer to low anonymity and waste in the use of pseudonyms. Our work searches to reduce the number of pseudonyms used per vehicle and to maintain the levels of anonymity of a synchronous strategy.

The remainder of this paper is organized as follows. Section 2 describes the main research related to the strategies adopted for pseudonym change in VANETs. Section 3 defines the main concepts of our proposal. Section 4 explains the planning of the simulations. Section V analyses the results. Finally, Section 5 presents the conclusions.

2. Related work

This section exposes the research related to pseudonym change strategies in VANET, only two of the researches focuses on the reputation of the vehicles. The authors of [7] propose a pseudonym change protocol based on the detection of trusted neighbours. The trusted term refers to the neighbour vehicles that are present within the vehicle's range in a minimum time, while in our strategy, it refers to vehicles with good reputation in a reputation system. The research [8] proposes a protocol that provides incentives to the vehicles that cooperate and change their pseudonyms when located in a mix-zone according to [9]. The reputation

of the vehicle increases when it cooperates, and the value of the increase depends on the number of vehicles than will be cooperating. In our research, the vehicle always cooperates in case of accomplishing with the condition of pseudonym.

Strategies where a vehicle decides to do individually the pseudonym change are simple to implement, but they have low anonymity and could perform ineffective pseudonym changes when the vehicle is alone. In [10], the pseudonym changes occur when a vehicle alters its direction and speed. The authors in [11,12] propose that a vehicle should update its pseudonym when the current density of neighbouring traffic is above a fixed threshold. The research in [13] develops a mechanism that considers factors such as the age of pseudonyms, speed, and moving direction of the vehicles.

Another individual strategy determines a fixed time (periodic) to change the pseudonym, instead of storing a very large number of pseudonyms, every vehicle keeps a set of pseudonyms (called a pseudonyms pool) which are used for specific time slots [14]. The length of the time slot determines how often a vehicle changes its pseudonym. The benefit of this strategy is that a vehicle always has a valid pseudonym even if the CA is not reachable. However, as soon as the attacker knows the period of pseudonym changing which is easy to discover, tracking becomes possible [15].

The random change strategy usually generates a random number before broadcasting a beacon. The pseudonym changes if the random number is below a threshold, which is set in advance [16]. As a result, an adversary cannot predict the next pseudonym change. In [17] an analytical model of the previous research is proposed to quantify its level of location privacy by calculating the size of the anonymity set of a vehicle with its neighbour. However, tracking is still possible if only one or a few vehicles change pseudonyms at a determined time.

In the researches [18,19], a vehicle changes the pseudonym when vehicles nearby are found with a similar status (as defined in 3.7). If the change is not successful, the system tries to change the pseudonym again, and in the worst scenario, the system may change pseudonyms continually, which results in more pseudonyms wasted. In addition, the simulations only took into account of partial information (i.e. the position of the vehicle) to deduce the number of neighbouring vehicles with similar status.

In [20], a vehicle can exchange pseudonyms with one of its neighbours that request it. This scheme requires the presence of an access point to forward the swap messages. In [21], the neighbours of a vehicle can choose to cooperate with it to change pseudonym depending on the expiration dates of their current pseudonyms. The request might cause a more asynchronous pseudonym change, and thus weaken the anonymity.

The synchronous strategy incorporates all the status information as defined in 3.7 and inserts a flag into the beacons to indicate if a vehicle is eligible to change its pseudonym, and consequently increase the probability of pseudonyms changing simultaneously [6,22]. It does

not validate whether the change of the pseudonym was successful or not. This prevents the vehicle from changing pseudonyms needless. In a synchronous strategy, when a vehicle meets the trigger, its neighbours may not meet the trigger as well. The authors of [23] establish a general framework of cooperation for pseudonyms changing, its purpose is to enable to the neighbours to change pseudonyms in the event of receiving a change flag. This mechanism increases the degree of anonymity, but require more effort and control.

3. Pseudonym change strategy

This section defines the concepts that form the building blocks of our strategy of pseudonym change: Public Key Infrastructure (PKI), processing time of the Elliptic Curve Digital Signature Algorithm (ECSDA), pseudonyms, pseudonym revocation, traceability problems, information about vehicular status, anonymity, reputation score, and reputation system.

3.1. Public Key Infrastructure (PKI)

The security architecture based on PKI relies on asymmetric encryption/decryption algorithms to provide several security services, such as certificate generation, renewal and revocation, signing and issuing, checking and auditing. The digital certificate accompanying the message signature is a countermeasure against different types of attacks in VANETs. This certificate provided by a CA in the PKI links a public key to the identification of the owner. A vehicle receives a digital certificate used to authenticate with third authorities in the network. A vehicle also receives a set of pseudonyms from the CA, which it will use to authenticate anonymously with other vehicles without revealing any identity.

Due to the limitations of computer power, memory, and connection time in VANET, the most acceptable PKI implementation is the Elliptic Curve Cryptography (ECC). Elliptic curve based systems can be implemented with smaller public key sizes than other digital signature algorithms (i.e., Rivest Shamir and Adleman/RSA, Diffie-Helman/DH and Digital Signature Algorithm/DSA). ECDSA offers the same level of resistance against the best currently known attacks than other algorithms, for example, an elliptic curve over a 256-bit field currently gives the same level of security as a 3072-bit RSA/DH/DSA. The difference becomes even more dramatic as the desired security level increases, e.g., 512-bit ECC is currently equivalent in security to 15,360-bit RSA/DH/DSA [24]. Furthermore, the IEEE and ETSI standards propose the use of the ECSDA for message authentication.

3.2. Processing time of ECSDA

The elliptical curve selected and the kind of processor incorporated into the vehicles influences on the processing time to exchange information quickly and safely between them. Table 1 lists the size of the ECDSA key, Secure Hash Algorithm (SHA) and curve recommended for signing and checking messages in compliance with the standards IEEE 1609[1], ETSI [25], and the guidelines of the National Institute of Standards and Technology (NIST) [26].

Table 1
ECDSA schemes for signing and verifying of messages.

Standard	ECDSA Key (bits)	SHA	Curve
IEEE 1609.2	224	224	secp224r1
ETSI TS 103 097	256	256	secp256r1
NIST-1	192	256	secp192r1
NIST-2	224	256	secp224r1
NIST-3	384	384	secp384r1

Source: The Authors.

The processing time (in ms) for signing and checking messages was measured in a computer with 2.66 GHz Intel Core 2 Quad processor, using ECC [4]. The research in [27] also measured the processing time using computers with Intel architectures Intel, of 1GHz and 3GHz, Table 2 compares the results; the experiments with a 3GHz processor obtained the lowest processing time. For instance, if we selected the standard ETSI which employs the secp256r1 elliptic curve, keys of 256 bits and SHA-256, the processing time to sign a message is 0.26 ms, and the processing time to check the message is 1.22 ms.

Table 2
Average cryptographic operation delay (ms) for the ECDSA.

ECDSA/Processor	1 GHz	2.66GHZ	3GHz
IEEE-Sign	5.84	3.22	0.35
IEEE-Verify	34.91	11.43	1.02
ETSI-Sign	6.17	4.03	0.26
ETSI-Verify	44.03	16.19	1.22
NIST-3-Sign	14.55	8.12	0.52
NIST-3-Verify	143.63	34.80	2.98

Source: The Authors.

3.3. Pseudonyms

Pseudonyms are short-term public key certificates that do not contain any information identifying the vehicle. The use of pseudonyms provides the property of unlinkability. The PKI scheme involves creating pseudonyms

and obtaining their keys from the CA, and then saving this cryptographic information in the Tamper Proof Device (TPD) or in the Trusted Platform Module (TPM) of the vehicles. The pseudonym refill in the vehicle may be offline or online. In offline, the CA sends all the data to the vehicle periodically, but this requires too much storage in the vehicle. In online, the vehicle downloads the data through RSUs when required [28].

The revocation of pseudonyms is necessary in the face of continuous misbehavior by a vehicle. There are two ways of dealing with this: Certificate Revocation List (CRL) and pseudonym update rate. The CRL must include all the peer's non expired pseudonyms public keys. The second method is to specify a pseudonym update rate so that the vehicles will quickly run out of certificates and will have to communicate with the CA to obtain more pseudonyms. In our implementation, the pseudonyms have an expiration date and the vehicles must frequently update pseudonyms.

3.4. Traceability problem

The use of a single pseudonym is not enough to protect privacy, in particular the property of untraceability. To address this problem, each vehicle possesses multiple pseudonyms that change frequently from one pseudonym to another [29,30]. The number of pseudonyms depends on the frequency of the changes, which ranges from seconds to hours. By increasing the frequency of pseudonyms changing, the chances of an intruder being able to launch a successful attack against privacy will be significantly reduced, but there will be a sharp increase in the amount of storage space needed to save pseudonyms [31].

The authors in [32] mention that although three vehicles may change their pseudonyms at the same time, the information about location and velocity embedded in safety messages can still provide information to an adversary to break the privacy. If the pseudonyms change in an incorrect way, an intruder is still able to link the current pseudonym to the next and its mobility trace can easily be disclosed [33]. Simply changing pseudonyms at an unappropriated time or with an improper status wastes pseudonyms and leads to an increase in the number of pseudonyms needed for a vehicle, and accordingly, more resources are required for storing or calculating them. In the case of VANETs with a large number of vehicles, it is a big challenge to handle such a huge number of pseudonyms.

3.5. Anonymity

The anonymity set of a vehicle includes the vehicle and its neighbours when they change pseudonyms together at the same place-time. The anonymity of a vehicle refers to the non-identification within the anonymity set. The strategies of pseudonym change seek to improve

this property. A truly anonymous system must remove any anonymity-compromising information, or at least make it less useful to an attacker.

3.6. Information about vehicular status

Each vehicle periodically broadcasts beacon messages openly to all of its neighbours. Beacons include information about vehicular status, such as velocity, position and heading direction. Two vehicles have a **similar status** if they have the same heading directions, velocities differ in terms of *vel m/s*, and the distance between them is less than *d - min m* [6]. This information is used by a pseudonym change strategy to determine the "change condition", i.e., if two or more vehicles have a **similar status** to achieve anonymity.

3.7. Reputation system

The main entities in the reputation system are Certificate Authority (CA) and Reputation Server (RS). The CA is a Trusted Third Part (TTP), which extends the functions of a traditional CA by issuing pseudonyms to the vehicles. The RS knows the identity of the vehicles, but has no knowledge of the pseudonyms issued to them by the CA. The RS can receive feedback with ratings, judging the behaviour of anonymous vehicles in VANETs. The RS maps the anonymous identities of the vehicles for the real ones, and updates the reputation scores.

3.7.1. Reputation score

The reputation of a vehicle depends on its ability to maintain a score that reflects its behaviour in the VANET. The reputation depends of the VANET application, the research in [34] proposes the composed reputation by including the behaviors of generating reliable messages and cooperating in the forwarding of messages. The reputation score (*Rep*) of a vehicle is the result of the aggregation of feedback by peer vehicles that evaluate its behaviour. In a centralised scheme, the RS is responsible for collecting feedback from the VANET, as well as computing and maintaining the global reputation scores of the vehicles [35]. In this paper, a Misbehaviour Vehicle (MV) is a vehicle that will always send fake messages, but it will also report the feedback of the peers correctly.

3.7.2. Reputation certificate

The Reputation Certificate (RC) is a certificate issued and signed by the Reputation Server. The RC contains the latest reputation score of the vehicle, which the RS keeps and updates based on the feedback supplied by the peer vehicles in the VANET. The vehicle updates its RC through an opportunistic contact with the RSU.

3.7.3. Reputation status

The Reputation Status of a vehicle, denoted as *RSt*, is a discrete approximation of the reputation score (*Rep*) maintained by the Reputation Server. An example of mapping the reputation score of 0.2 to *RSt* would be rounding off the decimal and getting a result of zero. A backward mapping from *RSt* score to the reputation score should be impossible. In our strategy, the beacons incorporate the Reputation Status assigned of one of two possible values. This is, *RSt* is assigned the value +1 for the vehicles with good reputation and -1 for the misbehaving vehicles. Thus, our strategy protects the anonymity of the vehicles due to the fact that the beacons do not reveal an identifiable reputation value.

3.7.4. Overall operational forecasted costs

The costs of the reputation system mainly include the operation and administration of the RS. Initially, the manufacturers of the vehicles and the Transit Regulatory Authority can cover these costs. In second place, the financial support will come from the Service Providers interested in selling products or services through the VANETs. The administration of main roads and service providers such as business owners or companies who have business alongside the main roads, might wish to advertise their services to the nearby vehicles and thus target many potential customers as in [36-38]. Financial entities such as banks, credit card companies, payment systems and insurance companies will also be interested in investing in new business involving VANETs, which handle sensitive information for reputation. Eventually, the vehicle owners will be able to contribute to a part of the registration costs and the annual renewal of the licence of the vehicle

3.8. Synchronous change strategy

In the strategy based on the synchronous pseudonym change proposed in [6], the beacons add a *change* flag, to announce that the vehicle is ready to change its pseudonym. The vehicle uses a current pseudonym for a time of 60s, and then the algorithm enables the *change* flag in the communications to indicate to the other vehicles that it plans to change the pseudonym. The minimum time represents a reasonable value for position based routing. After this, the system enters a *wait-check* sub cycle where it remains until it fulfils the change condition. This condition involves a minimum number of *K* neighbour vehicles with the *change* flag enabled and similar status. If the previous condition is not fulfilled, the vehicle waits for a maximum time of 60s to change the pseudonym. In this way, the system guarantees a minimum time of change between two pseudonyms.

3.9. Including the Reputation Status (RSt)

Our proposal is based on the synchronous strategy to achieve higher levels of anonymity than an individual strategy [6]. In VANETs, decision-making uses the reputation, such as forwarding or rejecting packets sent by a vehicle, regarding or disregarding it as an option in the routing of data, etc. [39]. Our strategy assumes that if there are no malicious vehicles around when the change condition triggers, there is no risk of tracking and consequently a pseudonym change is not necessary. We propose to add the information on the Reputation Status *(RSt)* of the neighbour vehicles to the parameters of evaluation of the condition of change, together with the similar status condition and the synchronisation with other vehicles, see Fig. 1. Thus, we consider at least one of them with a negative Reputation Status to enable the change. Our goal is to reduce the number of pseudonyms used per vehicle and to maintain the rate of success of the changes closer to the synchronous strategy.

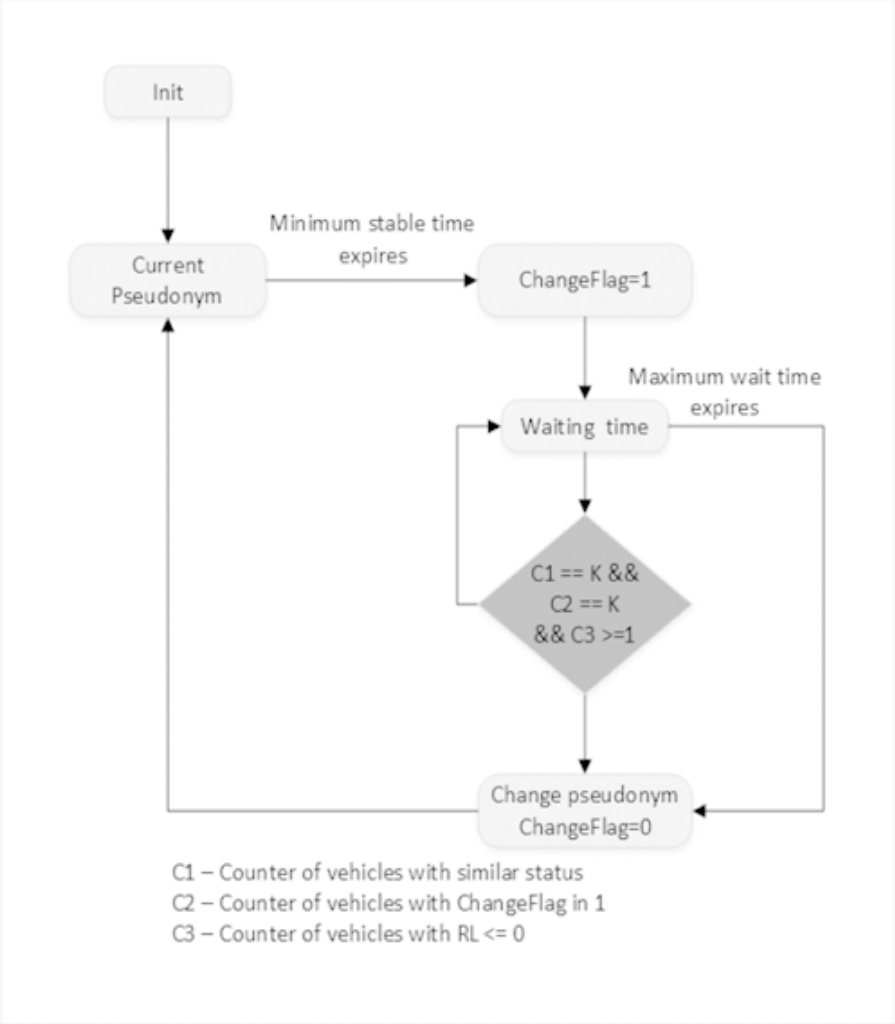

Figure 1
Pseudonym changing algorithm.
Source: The Authors.

4. Simulation setup

We simulated three pseudonyms-changing strategies: an individual strategy (similar status), the synchronous strategy, and including the Reputation Status of the vehicles. Tools used in this research: the mobility simulator SUMO [40], network simulator OMNET++ [41], the Vehicular environment in network simulation Veins [42] and the cryptographic library Crypto++ [43].

4.1. Simulation scenario

We selected a scenario built in the iTETRIS ("An Integrated Wireless and Traffic Platform for Real-Time Road Traffic Management Solutions") project [44]. The given data included representations of the areas around the "Andrea Costa" and the "Pasubio" roads [45]. The scenario included the traffic demand for Bologna's peak rush hour (8:00 am - 9:00 am) and the flow of vehicles in the scenario; in Fig. 2, 1843 vehicles enter the scenario, but not all them keep in it. In Fig 2, the line with squares represents the vehicles entering the scenario. The line with diamonds stands for the vehicles that going out to the simulated scenario. We see that the number of vehicles represented in these lines continues increasing minute by minute, and the number of vehicles going out is lower than the number entering. For these reasons, the line with triangles indicating the number of vehicles that stayed in the simulation is constant. It should be noted that about 600 vehicles per minute travel into the areas around the roads of the scenario.

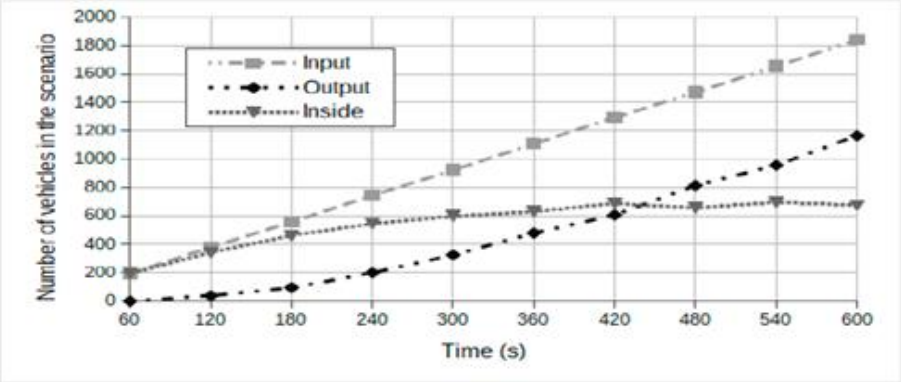

Figure 2
Number of vehicles in the Bologna scenario.
Source: The Authors.

4.2. Simulation parameters

Table 3 shows the main parameters of mobility and the network used in the simulations. We performed simulations for 600s and executed five runs for each experiment. At 600s, 1843 vehicles entered the scenario.

Table 3
Mobility, scenario, and network parameters.

Parameter	Value
Maximum velocity	50 km/h
Average velocity	28 km/h
Urban área	4.5 Km^2
Number of vehicles	1843
Transmission rate	6 Mbps
Communication range	250 m
MAC protocol	IEEE 802.11p
Network protocol	Wave Short Message Protocol
Beacon frequency	1 Hz
Simulation time	600s

Source: The Authors.

4.3. Planning of experiments

We incorporated the metrics, response variables and factors as defined below.

4.3.1. Metrics

The number of used pseudonyms: this refers to the total number of current pseudonyms attached to the vehicles as the result of the changing strategy;

The number of successfully changed pseudonyms: this refers to the total number of pseudonyms changed without risk of tracking;

The successful rate of changed pseudonyms: This refers to the total number of successfully changed pseudonyms with regard to the number of used pseudonyms;

Average time for pseudonym changing: this refers to the average of the maximum waiting time for the vehicles during the change of the pseudonym.

4.3.2. Fixed Factors

vel: this is the difference in speed between two vehicles defined by the status strategy, set to 0.5 m/s;

d - min: this is the distance between two vehicles defined by the status strategy, set to 20 m;

K: number of neighbours in the synchronous strategy with the change flag enabled set to 2;

Elliptic curve: this refers to the type of elliptic curve used to implement the functions of signing and verification of the pseudonyms; we selected the secp256r1 curve.

4.3.3. Variable Factors

Penetration Rate (PR): this refers to the ratio of the number of vehicles with communication modules installed with respect to the total number of vehicles in the simulation. This is because the VANETs will grow gradually until all the vehicles are fitted with wireless technology;

Pseudonym-change strategy: 1) *Status strategy* checks if the vehicles have a similar status, as defined in Subsection 3.6; 2) *Synchronous strategy* verifies both the simultaneity and vehicular status information for pseudonym change. Simultaneity is achieved when a number *K* of neighbouring vehicles enable the *change* flag [13]; 3) *Including the Reputation Status* in which the simultaneity, vehicular status information and the Reputation Status are taken into account for pseudonym change, as defined in Subsection 3.9;

Percentage of Malicious Vehicles (MV): this is the number of vehicles that have a negative Reputation Status with regard to the number of vehicles in the simulation.

A total number of 20 experiments were carried out and the *PR* ranged from 40% to 100% during the strategy of pseudonym changing. Three cases conducted for the proposed strategy were: 50%, 10% and 0% of MV. Table 4 shows the planned experiments.

Table 4
Mobility, scenario, and network parameters.

Experiment	*PR*	Strategy
1	100%	Status
2	100%	Synchronous
3	100%	Rep with 0% *MV*
4	100%	Rep with 10% *MV*
5	100%	Rep with 50% *MV*
6	80%	Status
7	80%	Synchronous
8	80%	Rep with 0% *MV*
9	80%	Rep with 10% *MV*
10	80%	Rep with 50% *MV*
11	60%	Status
12	60%	Synchronous
13	60%	Rep with 0% *MV*
14	60%	Rep with 10% *MV*
15	60%	Rep with 50% *MV*
16	40%	Status
17	40%	Synchronous
18	40%	Rep with 0% *MV*
19	40%	Rep with 10% *MV*
20	40%	Rep with 50% *MV*

Source: The Authors.

5. Results and discussions

This section exposes the results as follows a) the number of used pseudonyms, b) the number of successfully changed pseudonyms, c) the successful rate of changed pseudonyms, and d) the average time needed for the pseudonym change.

5.1. Effect of the strategies on the number of used pseudonyms

Fig. 3 compares the total number of used pseudonyms for the 1 to 4 experiments in Table 4. The experiments assumed a penetration rate of 100% and the strategies with status, synchronous, reputation with 0% *MV*, and reputation with 10% *MV*.

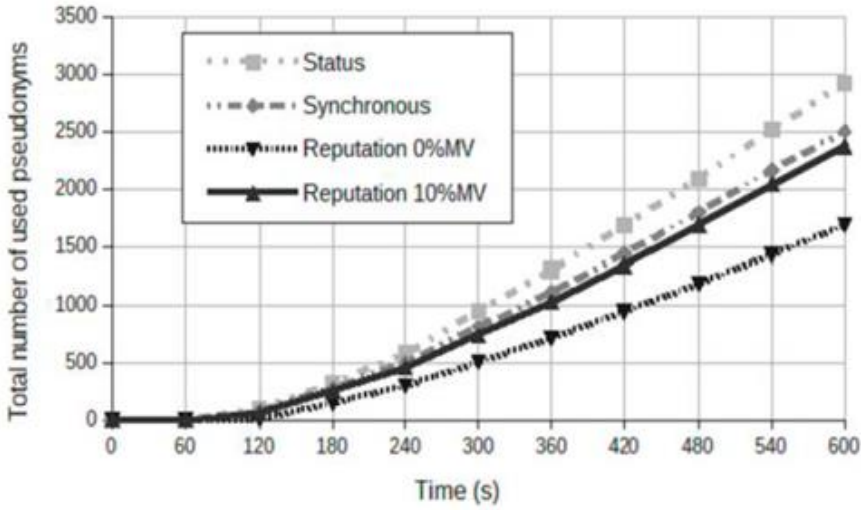

Figure 3
Comparison among strategies on the total number of used pseudonyms.
Source: The Authors.

The status strategy obtained the highest number of used pseudonyms because this strategy is able to find the conditions needed to change the pseudonym more quickly. In contrast, in the case of the strategy of *Rep* with 0% *MV* where there was an absence of misbehaving vehicles, the strategy did not change the pseudonyms until the maximum waiting time expired, as we expected. The results of the reputation strategy with 10% of *MV* were close to the results of the synchronous strategy. The main reason is that the number of misbehaving vehicles is low. Only 10% of the cases the strategy found the conditions for pseudonym change, and one of their neighbours had a negative reputation.

5.2. Effect of the strategies on the number of successfully changed

Fig. 4 compares the total number of successfully changed pseudonyms with the 1 to 4 experiments in Table 4. The experiments assumed a penetration rate of 100% and the strategies with status, synchronous,

reputation with 0% *MV*, and reputation with 10% *MV*. The status strategy had the lowest anonymity because the probability of changing pseudonyms simultaneously with other neighbouring vehicles was low. On the other hand, this probability increases with the synchronous strategy where the results with successfully changed pseudonyms were the highest.

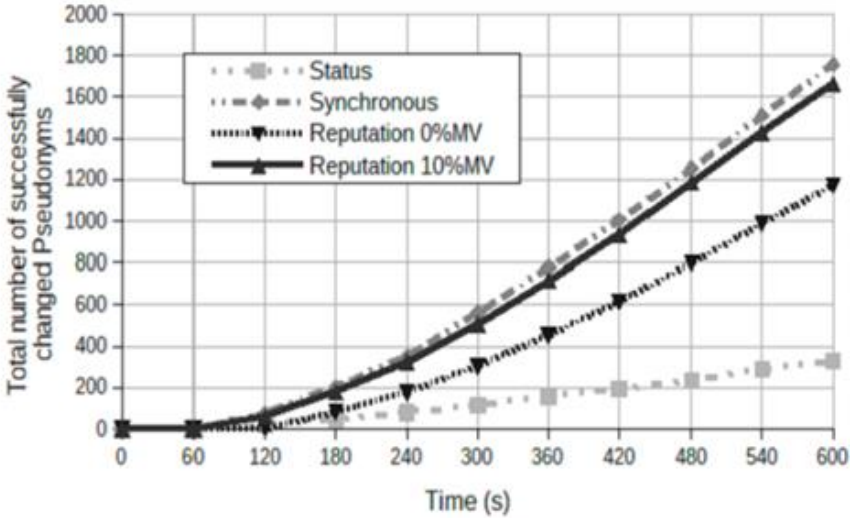

Figure 4
Comparison of the total number of successfully changed pseudonyms among the strategies.
Source: The Authors.

The results for the case with 10% *MV* are close to the results of the synchronous strategy due to the low number of misbehaving vehicles. The results for the case with 0% *MV* were higher than the results of the status strategy, and lower than the results of the synchronous strategy.

5.3. Effect of the strategies on the average time for pseudonym changes

Fig. 5 depicts the results of the average time to change pseudonyms for the 1 to 5 experiments in Table 4. The average time is higher for the reputation strategy (with 0%*MV*) than for the other strategies, which is almost 120s. These results do not put the tracking of the vehicles at risk, because the average time increases when in the reputation strategy, the neighbouring vehicles had a good reputation; moreover, the time for pseudonym change goes on until the maximum waiting time, i.e., 120s. Instead, when the reputation strategy has 10% *MV*, the average time decreases because some neighbouring vehicles have a bad reputation and the time for pseudonym change decreases. This time is close to the average time achieved by the synchronous strategy. In the reputation strategy, if the percentage of *MV* increases, the average time in the reputation strategy will be close to the results of the synchronous strategy because the number of pseudonyms used for both strategies was very similar, which was checked for the experiment 20 (with 50% *MV*) in Fig. 5.

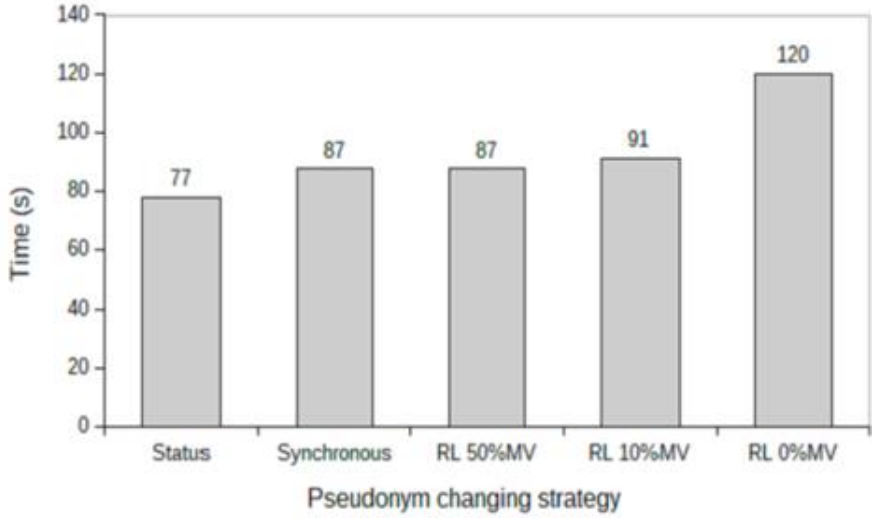

Figure 5
Comparison among strategies on the total number of used pseudonyms.
Source: The Authors.

5.4. Effect of the strategies on the number of successful rate of changing pseudonyms

Fig. 6 shows the results of a successful rate of pseudonyms change for all the 20 experiments in Table 4. The successful pseudonyms change rate for the reputation and synchronous strategy increases as the *PR* increases.

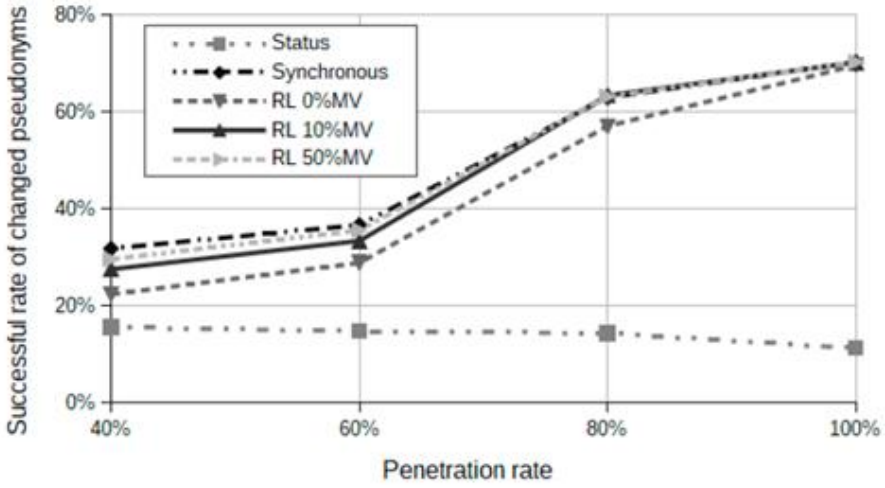

Figure 6
Successful rate of changed pseudonyms.
Source: The Authors.

In a dense scenario, such as that used in our simulations, even in the low penetration rate (40%), the results of the success rate of pseudonym change for the reputation and synchronous strategies are higher than for the status strategy. This is because, in the metrics, response variables and factors as defined below, the probability that at least two vehicles with similar status will change their pseudonym is higher. With 100% of *PR*,

the results for the synchronous and reputation strategies were similar to the success rates in about 70%.

In addition, Fig. 6 shows that for all the strategies except the status strategy, the results decrease as the *PR* increases because the number of events that satisfy the conditions of the pseudonym changes have risen and consequently, the number of pseudonyms wasted also increased. In the reputation strategy, if the percentage of MV increase, the success rate will be close to the results of the synchronous strategy because the number of pseudonyms wasted for both strategies were very similar as shown in Fig. 6.

6. Conclusions

Our work proposes to employ the Reputation Status of the neighbouring vehicles as additional input information for the pseudonym changing algorithm. Our strategy achieved a lower number of pseudonyms used was lower than in the others strategies. Thus, it optimises the storage resources of the vehicle at the same time that it guarantees the privacy properties. In the absence of misbehaving vehicles, the pseudonym changing goes on until the maximum waiting time. When the system detects a misbehaving vehicle and fulfil the condition of the trigger, the pseudonym is changed. Our results of the success rate of the pseudonym change with misbehaving vehicles were higher than with the individual strategy, and were lower than the synchronous strategy. However, the results without misbehaving vehicles were close to the results of the synchronous strategy.

References

[1] IEEE Vehicular Technology Society. IEEE Standard for wireless access in vehicular environments - security services for applications and management messages. IEEE std. 1609.2- 2013 (Revision of IEEE Std 1609.2-2013), March, pp. 1-240, 2016. DOI: 10.1109/IEEESTD.2016.7426684

[2] ETSI. Etsi ts 102 941 v1.1.1- Intelligent Transport Systems (ITS); security, trust and privacy management, Technical Report, 2012.

[3] De Fuentes, J.M., González-Tablas, A.I. and Ribagorda, A., Overview of security issues in vehicular ad-hoc networks. In: Handbook of research on mobility and computing: evolving technologies and ubiquitous impacts. IGI Global, 2011. pp. 894-911. DOI: 10.4018/978-1-60960-042-6.ch056

[4] Santos-Jaimes, L.M., Ullah, K. and Moreira, E dos S., A secure commercial ads dissemination scheme for vehicular networks, Proceedings of 8th IEEE Latin-American Conference on Communications (LATINCOM). Medellín: IEEE, [online]. 2016. Available at: https://ieeexplore.ieee.org/document/7811610/. DOI: 10.1109/LATINCOM.2016.7811610

[5] Santos-Jaimes, L.M, Ullah, K. and Moreira E dos S., ARS: anonymous reputation system for vehicular ad hoc networks. Proceedings of 8th IEEE Latin-American Conference on Communications (LATINCOM). Medellín: IEEE, [online]. 2016. Available at: https://ieeexplore.ieee.org/document/7811600/. DOI: 10.1109/LATINCOM.2016.7811600

[6] Liao, J. and Li, J., Effectively changing pseudonyms for privacy protection in vanets. In: 10th International Symposium on Pervasive Systems, Algorithms, and Networks. Kaohsiung: IEEE, [online]. 2009, pp. 648-652, Available at: https://ieeexplore.ieee.org/document/5381686/.

[7] DOI: 10.1109/I-SPAN.2009.103

[8] Moghraoui, K. and Amar-Bensaber, B., An efficient pseudonym change protocol based on trusted neighbours for privacy and anonymity in VANETs. Proceedings of the 5th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications. Cancun, ACM, [online]. 2015, pp. 93-99. Available at: https://dl.acm.org/citation.cfm?doid=2815347.2815355. DOI: 10.1145/2815347.2815355

[9] Ying, B. and Makrakis, D., Reputation-based pseudonym change for location privacy in vehicular networks. Proceedings of International Conference on Communications (ICC). London: IEEE, [online]. pp. 7041-7046, 2015. Available at: https://ieeexplore.ieee.org/document/7249449/. DOI: 10.1109/ICC.2015.7249449

[10] Ying, B., Makrakis, D. and Mouftah, H.T., Dynamic mix-zone for location privacy in vehicular networks. IEEE Communications Letters, 17(8), [online]. pp. 1524-1527, 2013. Available at: https://ieeexplore.ieee.org/document/6560048. DOI: 10.1109/LCOMM.2013.070113.122816

[11] Li, M., Sampigethaya, K., Huang, L., et al., Swing & swap: user-centric approaches towards maximizing location privacy. Proceedings of the 5th ACM workshop on Privacy in electronic society. Alexandria: ACM, [online]. pp. 19-28, 2006. Available at: https://labs.ece.uw.edu/nsl/papers/WPES-2006.pdf. DOI: 10.1145/1179601.1179605

[12] Chaurasia, B.K. and Verma, S., Optimizing pseudonym updation for anonymity in vanets. Proceedings of Asia-Pacific Services Computing Conference APSCC'08. Yilan: IEEE, [online]. pp. 1633-1637, 2008. Available at: https://ieeexplore.ieee.org/document/4780916/. DOI: 10.1109/APSCC.2008.110

[13] Chaurasia, B.K., Verma, S., Tomar, G.S., et al., Pseudonym based mechanism for sustaining privacy in vanets. Proceedings of First International Conference on Computational Intelligence, Communication Systems and Networks. Indore: IEEE, [online]. pp. 420-425, 2009. Available at: https://ieeexplore.ieee.org/document/5231877/. DOI: 10.1109/CICSYN.2009.79

[14] Chen, Y.S., Lo, T.T., Lee, C.H., et al., C. Efficient pseudonym changing schemes for location privacy protection in VANETs. Proceedings of International Conference on Connected Vehicles and Expo (ICCVE). Las Vegas: IEEE, [online]. pp. 937-938, 2013. Available at: https://ieeexplore.ieee.org/document/6799933/. DOI: 10.1109/ICCVE.2013.6799933

[15] Eckhoff, D., Sommer, C., Gansen, T., et al., Strong and affordable location privacy in vanets: Identity diffusion using timeslots and swapping. Proceedings of Vehicular Networking Conference (VNC). Jersey: IEEE, [online]. pp. 174-181, 2010. Available at: https://ieeexplore.ieee.org/document/5698239/. DOI: 10.1109/VNC.2010.5698239

[16] Ishtiaq-Roufa, R.M., Mustafaa, H., Travis-Taylora, S.O., et al., Security and privacy vulnerabilities of in-car wireless networks: A tire pressure

monitoring system case study. Proceedings of 9th USENIX Security Symposium. Washington DC: pp. 11-13, 2010.

[17] Pan, Y., Li, J., Feng, L., et al., An analytical model for random changing pseudonyms scheme in vanets. Proceedings of International Conference on Network Computing and Information Security (NCIS). Guilin: IEEE Computer Society, pp. 141-145, 2011. DOI: 10.1109/NCIS.2011.127

[18] Pan, Y., Li, J., Feng, L., et al., An analytical model for random pseudonym change scheme in VANETs. Cluster Computing. 17(2), pp. 413-421, 2014. DOI: 10.1007/s10586-012-0242-7

[19] Gerlach, M., Assessing and improving privacy in vanets. In: ESCAR, Embedded Security in Cars. 2006. DOI:10.1.1.84.8167&rep=rep1&type=pdf

[20] Gerlach, M. and Guttler, F., Privacy in vanets using changing pseudonyms ideal and real. Proceedings of 65th Vehicular Technology Conference- VTC2007-Spring. Dublin: IEEE, [online]. pp. 2521-2525, 2007. Available at: https://ieeexplore.ieee.org/document/4212947/. DOI: 10.1109/VETECS.2007.519

[21] Li, M., Sampigethaya, K., Huang, L., et al., Swing & swap: user-centric approaches towards maximizing location privacy. Proceedings of the 5th ACM workshop on Privacy in electronic society ACM, pp. 19-28, 2006. DOI: 10.1145/1179601.1179605

[22] Freudiger, J., Manshaei, M.H., Le- Boudec, J.Y., et al., On the age of pseudonyms in mobile ad hoc networks. Proceedings of IEEE INFOCOM. San Diego: IEEE, [online]. pp. 1-9, 2010. Available at: https://ieeexplore.ieee.org/document/5461975/. DOI: 10.1109/INFCOM.2010.5461975

[23] Liao, J., Li, J. and Pan, Y., Cooperatively changing pseudonyms for privacy protection in vanets. Proceedings of the 2nd IEEE international conference on wireless access in vehicular environments (WAVE). Shanghai, pp. 13-8, 2009. DOI: 10.1109/I-SPAN.2009.103

[24] Pan, Y. and Li, J., Cooperative pseudonym change scheme based on the number of neighbors in vanets. Journal of Network and Computer Applications. 36(6), pp. 1599-1609, 2013. DOI: 10.1016/j.jnca.2013.02.003

[25] Lauter, K. The advantages of elliptic curve cryptography for wireless security. IEEE Wireless communications. 11(1), pp. 62-67, 2004. DOI: 10.1109/MWC.2004.1269719

[26] ETSI. Intelligent Transport Systems (ITS), security, security header and certificate formats. Technical Report. ETSI TS 103 097, 2015.

[27] Turner, S., Housley, R., Polk, T., et al., Elliptic curve cryptography subject public key information. RFC 5480, 2009.

[28] Hamida, E.B., Noura, H. and Znaidi W., Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic countermeasures. Electronics. 4(3), pp. 380-423, 2015. DOI:10.3390/electronics4030380

[29] Ma, Z., Kargl, F. and Weber M., Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications. Proceedings of 68th Vehicular Technology Conference VTC. Calgary: IEEE, [online]. pp. 1-5, 2008. Available at: https://ieeexplore.ieee.org/document/4657287/. DOI: 10.1109/VETECF.2008.455

[30] Beresford, A.R. and Stajano, F., Mix zones: user privacy in location aware services. Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. Orlando: IEEE, [online]. pp. 127-131. 2004. Available at: https://ieeexplore.ieee.org/document/1276918/. DOI:10.1109/PERCOMW.2004.1276918

[31] Freudiger, J., Raya, M., Félegyházi, M., et al., Mix-zones for location privacy in vehicular networks. Proceedings of ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS). Vancouver: Infoscience, 2007. DOI: 10.1109/ACCESS.2018.2800907

[32] Alexiou, N., Laganà, M., Gisdakis, S., et al., Vespa: vehicular security and privacy-preserving architecture. Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. New York: ACM, [online]. pp. 19-24, 2013. Available at: https://dl.acm.org/citation.cfm?doid=2463183.2463189. DOI:10.1145/2463183.2463189

[33] Lu, R., Lin, X., Luan, T. H., et al., Pseudonym changing at social spots: an effective strategy for location privacy in vanets. IEEE transactions on vehicular technology. [online]. 61(1), pp.86-96, 2011. Available at: https://ieeexplore.ieee.org/document/5960806/. DOI: 10.1109/TVT.2011.2162864

[34] Buttyán, L., Holczer, T. and Vajda, I., On the effectiveness of changing pseudonyms to provide location privacy in vanets. Proceedings of European Workshop on Security in Ad-hoc and Sensor Networks. Berlin: Springer, pp. 129-141, 2007. DOI: 10.1007/978-3-540-73275-4_10

[35] Santos-Jaimes, L.M. and Moreira, E., An evaluation of reputation with regard to the opportunistic forwarding of messages in VANETs. EURASIP Journal on Wireless Communications and Networking. 2019(1), pp. 1-14, 2019. DOI: 10.1186/s13638-019-1518-x

[36] Vanni-P., R.M., Santos-J., L.M., Mapp, G., et al., Ontology driven reputation model for vanet. Proceedings of AICT 2016, The Twelfth Advanced International Conference on Telecommunications. Barcelona: IARIA, pp. 14-19, 2016.

[37] Yokoyama, R.S., Kimura, B.Y., Santos-J, L.M., et al., A beaconing-based opportunistic service discovery protocol for vehicular networks. Proceedings of 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA). Victoria: IEEE, [online]. pp. 498-503, 2014. Available at: https://ieeexplore.ieee.org/abstract/document/6844686/. DOI: 10.1109/WAINA.2014.82

[38] Ullah, K., Santos-J., L.M., Yokoyama, R.S., et al., Advertising roadside services using vehicular ad hoc network (vanet) opportunistic capabilities. Proceedings of 4th International Conference on Advances in Vehicular Systems, Technologies and Applications. Julians: IARIA, pp. 7-13, 2015.

[39] Ullah, K., Santos-J., L.M., Ribeiro, J.B., et al., Sadp: a lightweight beaconing-based commercial services advertisement protocol for vehicular ad hoc network. Proceedings of International Conference on Ad-Hoc Networks and Wireless. Lille: Springer, pp. 279-293, 2016. DOI:10.1007/978-3-319-40509-4_20

[40] Bidóia, M.C., Cavenaghi, M.A., Spolon, R., et al., Simulation of a centralized reputation system for vanets. Proceedings of International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA). The Steering Committee of the World Congress

in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2014.

[41] German Aerospace Center, Institute of Transportation Systems. SUMO Simulation of Urban Mobility [online]. [Consulted in: June of 2018]. Available at: Available at: http://sumo.dlr.de/index.html

[42] OpenSim Ltd., Omnet++ discrete event simulator. [online]. [Consulted in: June of 2018]. Available at: Available at: https://omnetpp.org/

[43] Christoph Sommer. The open source vehicular network simulation framework [online]. [Consulted in: June of 2018]. Available at: Available at: http://veins.car2x.org/

[44] Crypto++ community. Crypto++ library 5.6.5 [online]. [Consulted in: June of 2018]. Available at: Available at: http://www.cryptopp.com/

[45] Bieker, L., Krajzewicz, D., Morra, A., et al., Traffic simulation for all: a real world traffic scenario from the city of bologna. Proceedings of Modeling Mobility with Open Data, 2nd SUMO Conference. Berlin, Springer, pp. 47-60, 2015. DOI:10.1007/978-3-319-15024-6_4

[46] German Aerospace Center (DLR). Data scenarios. Bologna [online]. [Consulted in: June of 2018]. Available at: Available at: https://sumo.dlr.de/docs/Data/Scenarios.html#bologna

Notes

L.M. Santos-Jaimes, received the BSc. in Systems Engineering from the University Francisco de Paula Santander, Colombia in 1996, the MSc. in Systems and Computation Engineering from the University of the Andes, Colombia, in 1999, and the PhD. degree in Sciences from the University of São Paulo, Brazil in 2017. She is titular professor and researcher with the Department of Electric, Electronic, Telecommunications and Systems, University of Pamplona, Colombia. Her research interests include vehicular networks, wireless networks, network security, privacy, mobile applications, Internet of Things, and IPv6. ORCID: 0000-0003-4499-795X

E. dos S. Moreira, received the BSc in Electrical Engineering from the University of São Paulo, São Paulo, Brazil, in 1982, the MSc in physics from the University of São Paulo, Brazil in 1984, and the PhD. degree in Computer Science from the University of Manchester, Manchester, U.K., in 1989. He conducted post-doctoral studies at Strathclyde University Glasgow Scotland, in 1993 and at the Computer Laboratory, University of Cambridge from 2007 to 2006. He is a full professor and researcher at the Instituto de Ciências Matemáticas e de Computacão (ICMC), University of São Paulo. His current research interest include computer networking, secure wireless communication, mobility management, and Internet technology. ORCID: 0000-0002-7035-1717

How to cite: Santos-Jaimes, L.M. and Moreira, E. dos S, Pseudonym change strategy based on the reputation of the neighbouring vehicles in VANETs. DYNA, 86(211), pp. 157-166, October - December, 2019.