SDN-based Pseudonym-Changing Strategy for Privacy Preservation in Vehicular Networks

Abdelwahab Boualouache, Ridha Soua, and Thomas Engel
SnT, University of Luxembourg, Luxembourg
Email: {abdelwahab.boualouache, ridha.soua, thomas.engel}@uni.lu

***Abstract*—The pseudonym-changing approach is the de-facto location privacy solution proposed by security standards to ensure that drivers are not tracked during their journey. Several Pseudonym Changing Strategies (PCSs) have been proposed to synchronize Pseudonym Changing Processes (PCPs) between connected vehicles. However, most of the existing strategies are static, rigid and do not adapt to the vehicles' context. In this paper, we exploit the Software Defined Network (SDN) paradigm to propose a context-aware pseudonym changing strategy (SDN-PCS) where SDN controllers orchestrate the dynamic update of the security parameters of the PCS. Simulation results demonstrate that SDN-PCS strategy outperforms typical static PCSs to perform efficient PCPs and protect the location privacy of vehicular network users.**

***Index Terms*—Vehicular networks; Location privacy; Pseudonym Changing; Context-aware; Software Defined Network (SDN).**

I. Introduction

Vehicular services and applications such as collision avoidance, cooperative driving and traffic management rely on the periodic broadcast of safety-related messages, known as beacons. The main goal of these beacons is to establish cooperative awareness between vehicles [1]. However, these beacons carry sensitive information such as position, speed, velocity, and heading which may threaten the location privacy of vehicles' users. Indeed, these messages could easily be eavesdropped by a passive adversary who can link these messages with their corresponding vehicles' identifiers and track the trajectory of the vehicle during its journey, which violate the location privacy of drivers [2].

The de facto solution to avoid tracking vehicles from their transmitted beacons is the use of multiple temporary identifiers, called pseudonyms, which are obtained from the Certification Authority (CA) and use them in succession [3]. When all pseudonyms in this set have been used, the vehicle can request a new pseudonym set from the CA. This solution, called the Pseudonym-Changing Strategy (PCS), is already part of the security standards of connected vehicles such as IEEE 1609.2 [4] and ETSI 102941-v1.1.1 [5]. PCSs aim to determine the best way for vehicles to change their pseudonyms in order to guarantee the unlinkability between them. However, as demonstrated by several studies, this approach fails to provide the required location privacy protection due to pseudonym linking attacks [6]. For this reason, many PCSs have been proposed to prevent this attack. These can be classified into two categories [6]: (i) Mix-Zone-based strategies: where vehicles change their pseudonyms on predefined road areas, called mix zones, and (ii) Mix-Context-based strategies: where each vehicle independently determines where and when to change its pseudonym. However, most of the proposed PCSs are static, rigid and do not adapt to the context of the vehicles. Once the security parameters of a given strategy are configured, they cannot dynamically be reconfigured according to a given situation or context such as the power of adversary, the traffic density, and the mobility pattern. For instance, the European standard ETSI TS 102 867 recommends changing a pseudonym every five minutes while the American SAE J2735 standard recommends changing it every 120 s or 1 km.

To address these issues, we exploit the Software Defined Networking (SDN) paradigm, which promises to bring programmability and flexibility to future vehicular networks. SDN provides a logically-centralized approach and decouples the control plan from the data plane to efficiently manage the network [7]. We then propose a new SDN-based pseudonym changing strategy called, SDN-PCS. The strategy is built on a hierarchical software defined vehicular network architecture and supports both infrastructure-based and infrastructureless scenarios. The strategy uses SDN controllers as strategy coordinators and relies on them to change the security parameters of the pseudonym-changing strategy. The security parameters in SDN-PCS are dynamically updated to perform efficient and effective pseudonym-changing processes (PCPs). The remainder of this paper is organized as follows. Section II describes some related work. The considered system and adversary model are presented in section III. The proposed SDN-based pseudonym-changing strategy is described in Section IV. The performance evaluation results are given in Section V. Finally, Section VI concludes the paper.

II. Related Work

Over the last few years, several PCSs have been proposed to prevent the pseudonym linking attacks. These strategies are classified into two categories [6]: (i) Mix-zone-based strategies, and (ii) Mix-context-based strategies. In the former, the PCP only occurs on predefined road areas, called mix zones. Freudiger et al. [8] proposed installing Cryptographic Mix zones on road intersections where all safety messages are encrypted. In [9] authors performed PCS at Social Spots such as signal-controlled intersections and parking lots. Boualouache and al. (a) [10][11] proposed stopping broadcasting safety

messages at signal-controlled intersections only while the traffic signal is red. These zones are called silent mix zones. The authors of [12] designed a roadside infrastructure, called the Vehicular Location Privacy Zone (VLPZ), which is similar to existing roadside infrastructures such as gas stations, electric vehicle charging stations, and toll booths.

Additional interesting PCSs are proposed in the mix-context-based category. These strategies can be executed everywhere, whenever the predefined context is identified. The study [13] considered the direction and the number of vehicles within communication range as mix context parameters. The vehicle changes its pseudonym only if it detects k neighboring vehicles, which are located at a distance smaller than the minimum distance and having a direction similar to it. Liao et al. [14] added the speed, the distance between vehicles and the road segment into the mix context. They also proposed inserting a bit (flag) in the safety message to indicate the willingness of a vehicle to change its pseudonym. The vehicle then changes its pseudonym if it finds k neighboring vehicles that have a similar status and whose flag is equal to 1. The authors of [15] introduced random encryption periods (REPs). When the vehicle decides to change its pseudonym, it sends a request to its neighbors to start a REP. During a REP, the safety messages are encrypted using a shared group key. Boualouache et al. [16] proposed the Traffic-Aware PCS, where vehicles continuously monitor road traffic status to find optimal locations where a silent mix zone can be created.

The mix-context-based PCSs are more practical, since vehicles can change their pseudonyms at any location if the predefined context is satisfied. However, the security parameters of mix-context strategies cannot be dynamically updated to take into account the dynamicity of the network. Recently, many SDN-based solutions have been proposed for vehicular networks. Huang et al. [17, 18] proposed a new three-plane architecture, which relies on SDN to provide efficient pseudonym resources management. The SDN control plane is responsible for deciding how the pseudonym resources forward among the pseudonym pools and for defining the corresponding rules. However, the authors do not describe how the pseudonyms are changed and which PCS is applied to prevent the linkability of pseudonyms.

III. System Architecture and Adversary Model

Here we describe our SDN vehicular network architecture and give some assumptions. We then present the adversary model and define the privacy level for vehicles.

A. Vehicular system model and assumptions

We consider a hierarchical SDN vehicular network architecture similar to the one proposed in [19]. We also assume that vehicles periodically form clusters that change over time. The clustering helps to reduce radio interference and overhead and to provide better support for density and mobility. In addition, as the cluster head (CH) will play the role of a local SDN controller, the clustering method implemented by the global SDN controller should then ensure the maximum stability of

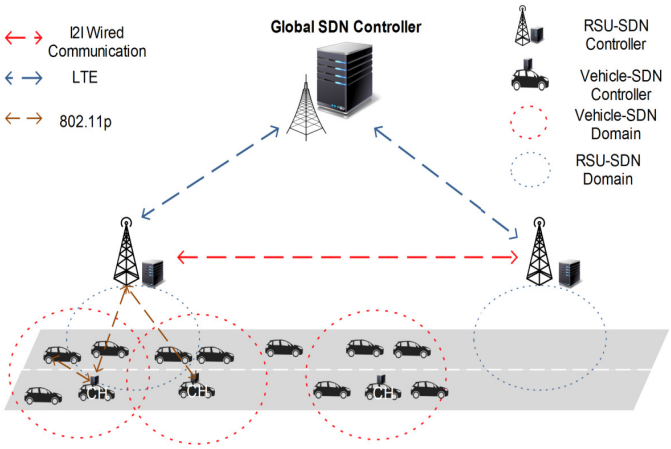


Fig. 1: Software defined vehicular network architecture

the CH to minimize how often the CH, and hence the local SDN controller, is changed. As illustrated in Figure 1, there are three SDN control levels in our architecture. The first is a local SDN that operates at the level of the cluster and which coordinates the PCS inside the cluster. This local SDN controller is called Vehicular-SDN Controller (VSDNC), and its cluster is called the VSDNC domain. The second level of the control is at Road-Side Units (RSUs). Each RSU includes an SDN controller and has its own control domain. The RSU-SDN Controller (RSDNC) coordinates different vehicular clusters that are within its range. Finally, the third level is the global SDN controller, which has global knowledge about the vehicular network. The remainder of the vehicles belong to the forwarding plane. Each vehicle is equipped with an IEEE 802.11p interface to communicate with other vehicles and with RSUs. An SDN controller and an SDN agent are also installed in each vehicle. While the SDN agent should be always activated, the SDN controller is initially deactivated and will only be activated when the vehicle becomes a CH and deactivated again if the vehicle reverts to being a cluster member. The internal clocks of vehicles are synchronized using GPS signals. Each RSU is also equipped with two interfaces: wired link to communicate with the neighboring RSUs, and an LTE interface to communicate with the global SDN controller. This latter is hosted at a distant location. We assume that the communication links between the VSDNC, the vehicles, and between the three types of SDN controllers are secured.

Each vehicle periodically broadcasts a safety message, where each message includes the location, a timestamp, the velocity and a content. Before joining the network, each vehicle registers with the CA. During registration, each vehicle V_i is pre-loaded with a set of m pseudonyms $K_{i,k}$ where $k \in \{1,..., \text{m}\}$, which are public keys certified by the CA. For each pseudonym $K_{i,k}$ of a vehicle V_i, the CA provides a certificate $Cert_{i,k}(K_{i,k})$. The safety messages are properly signed by the private key $K_{i,k}^{-1}$ corresponding to the

pseudonym $K_{i,k}$ to ensure the authentication. A certificate is attached to each message to enable other vehicles to verify the sender's authenticity.

B. Adversary Model

In this work, we assume an external passive adversary who aims to track the trajectory of target vehicle by eavesdropping all communications of any vehicle within a region of interest. We only consider syntactic attacks and not semantic attacks [6]. The adversary is not able to perform tracking using cameras, because the cost of global eavesdropping with cameras is much higher than radio-based eavesdropping. Consequently, camera-based global eavesdropping is beyond the scope of this work. The power of the adversary has a direct impact on the location privacy level of vehicles. If the adversary is strong then the level of location privacy may rapidly decrease following the PCS. The location privacy level can be expressed as function of the power of the adversary using the model proposed in [20]. Indeed, the loss of location privacy of a given vehicle v_i can be modeled using a function $S_i(t, T_i^c) : (\mathbb{R}^+, \mathbb{R}^+) \rightarrow \mathbb{R}^+$ where T_i^c is the time of the most recent pseudonym change of the vehicle v_i. The privacy loss increases with time according to a sensitivity parameter, $0 < \lambda_i < 1$ until it reaches a maximum value $G_i(T_i^c)$, which is the location privacy protection level achieved at last pseudonym change of v_i. It is set to 0 each time v_i changes its pseudonym. The privacy loss function can then expressed as follows:

$$S_i(t, T_i^c) = \begin{cases} \lambda_i(t - T_i^c) & \text{for } T_i^c \leq t < T_i^{max} \\ G_i(T_i^c) & \text{for } t \geq T_i^{max} \end{cases}$$

Where $T_i^{max} = \frac{G_i(T_i^c)}{\lambda_i} + T_i^c$ is the time when the function reaches the maximal privacy loss. The location privacy level of v_i at time t is given as follows:

$$G_i(t) = G_i(T_i^c) - S_i(t, T_i^c), t \geq T^c$$

IV. SDN-based Pseudonym Changing Strategy

Here we describe the main steps of our proposed SDN-based PCS: (i) the installation of the security parameters of the PCS, (ii) the local SDN monitoring and the PCP, and finally (iii) the dynamic changing of the PCS security parameters.

A. Installation of PCS security parameters

This step installs the PCS's security parameters in each SDN-controller and each vehicle. First, the global SDN controller installs the default PCS security parameters. However, these parameters will be dynamically updated by the SDN controller to adapt to security changes that have occurred. As shown in Figure 2, after the creation of the vehicular clusters, the global SDN controller sends the security parameters of the PCS to RSDNCs. Each RSDNC installs these security parameters as soon as it receives them. It will then send back an acknowledgment to the global SDN controller and forwards these security parameters to each VSDNC within its transmission rage. However, in the case of the infrastructure-less scenario, the VSDNC may be outside the range of the RSDNC. For this reason, we assume that a set of default PCS security parameters are already installed at the VSDNC. These parameters will be updated as soon as the VSDNC is in range of a RSDNC. Each VSDNC will then install the PCS security parameters and send back an acknowledgment to RSDNC. Finnaly, it sends the necessary PCS security parameters to each cluster member and starts the monitoring step.

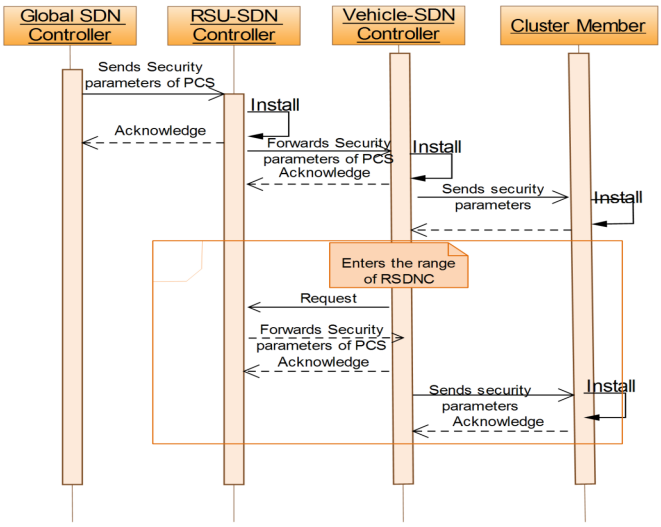


Fig. 2: Installation of PCS security parameters.

The following security parameters are considered by the proposed PCS:

- The threshold of privacy (α): the threshold below which the vehicle should change its pseudonym.
- The frequency of changing of pseudonyms (β): defines the number of pseudonyms that will be used each hour.
- The number of required vehicles (γ): defines the number of candidate vehicles required to initiate the PCP.
- The strategy timeout (δ): defines the duration after which the PCP should be initiated.

B. Monitoring and pseudonym-changing process

In this step, the local SDN controllers (VSDNCs) start monitoring the clusters to check whether the conditions are met to initiate the PCP. These conditions are defined by the previously installed PCS security parameters. The VSDNCs also inform the global SDN controller about the result of the PCP. This information will be used to update the security parameters, as described in the next paragraph. Moreover, each SDN-agent belonging to the forwarding plane, periodically sends an update to its VSDNC. These updates generally include the mobility parameters (position, speed, and acceleration) of vehicles and their current privacy level. These updates are used by VSDNCs to select the vehicles that can participate in the next the PCP. We exploit the safety messages to send these

updates. The mobility parameters are by default sent within the beacons and the extension fields are used to send the current privacy level of vehicles as described in [21].

A vehicle v_i is selected to participate in the next process of changing of pseudonym, only if the vehicle meets a specific context. The context is defined by the PCS security parameters that are forwarded by the global SDN controller. It principally includes the threshold of privacy, the number of required vehicles, and the strategy timeout.

Algorithm 1: Initiation of the PCS process

```
Data: An update from a vehicle v_i
Result: PS Strategy initiation
Initialize;
if (v_i.privacy level < α) then
    Add v_i to the list of participating vehicles (L);
else
    if (size of L = γ) then
        Initiate PCS process;
        Set the strategy timeout parameter (δ);
    end
end
```

As shown in the Algorithm 1, a vehicle v_i is added to the list (L) of vehicles that will participate in the next process of changing of pseudonyms, only its privacy level is below the privacy threshold parameter (α). If the number of vehicles included in L equals the number of required vehicles (γ) and the strategy timeout is not yet expired, the PCP is initiated. The strategy timeout (γ) should also be initialized after the initiation of PCS process. When the PCS process is initiated, the VSDNC sends a command to all the selected cluster members to change their pseudonyms simultaneously at a given time t. The whole PCS process is controlled by the VSDNC. The new privacy levels of vehicles participating in the PCS process will be calculated by the VSDNC following the end of this step.

C. Update of security parameters

The SDN controllers operating at the three levels of the control plane exchange information to ensure the efficiency of the applied PCS. Each VSDNC reports information to its regional domain controller (RSDNC) in order to keep track of vehicles changing their clusters. In addition, VSDNCs report information about the efficiency of the applied PCS to the global SDN controller via the RSDNs. The purpose of this information is to tune the PCS security parameters in order to obtain better location privacy protection. The PCS security parameters can be tuned as follows:

- The frequency of changing of pseudonyms (β): a higher frequency value has a positive impact on the location privacy. However, higher change frequency can have negative impacts on the application performance and will increase the number of pseudonyms used. Consequently, large amount of memory may be needed to store these pseudonyms. This parameter should thus carefully be turned by the global SDN controller according to the power of the adversary.
- The threshold of privacy (α): this parameter could also be tuned by the global SDN controller according to preferred levels of privacy protection, which are provided by users. For instance, this parameter could regularly be calculated based on the average preferred levels of privacy protection. This parameter could also be impacted by the power of the adversary. Indeed, the recommended threshold of privacy should dynamically be increased or decreased according to the power of the adversary.
- The number of required vehicles (γ): a high number of vehicles changing their pseudonym together has a positive impact on location privacy protection. However, as long as, the decision to initiate a PCS process depends on obtaining a required number of vehicles, the PCS may not perform well if this parameter is not well tuned. This parameter directly depends on the number of cluster members and their privacy level compared to the threshold of privacy. The global SDN controller should thus tune this parameter according to the information received from VSDNCs.
- The strategy timeout (δ): this parameter is closely related to γ parameter. It ensures that the PCS is executed even if the number of required vehicles is not achieved. This parameter should be tuned to prevent executing unnecessary iterations of the PCS.

V. Performance Evaluation

We simulate our SDN-PCS scheme using Veins, an inter-vehicular communication simulation framework based on two well established simulators OMNet++ [22] and SUMO.[23]. Table II summarizes the parameters considered in our simulations.

TABLE I: Simulation Parameters

Parameter	Value
Simulation duration	60 s
Transmission Range	500 m
Number of vehicles	30
The privacy threshold (α)	5
The frequency of PC (β)	30 s
The sensitivity parameter (λ)	0.4, 0.5,0.6s^{-1}
The default value of γ	10
The default value of δ	5 s

We consider the case of a highway. We simulate a two-lane straight road section of 1.5 Km. We focus on the impact of the proposed strategy on a given cluster. The privacy level values of vehicles are initialized using a normal distribution $\mathcal{N}$ (μ,σ) with a mean equal to μ = 8 and with a standard deviation equals to σ = 5/3. In addition, as shown in Table II, fixed values are used to initialize some of the security parameters such as the privacy threshold (α), the frequency of pseudonym changing (β). However, other security parameters such as

TABLE II: SDN-PCS vs static PCS: Statistics on the preformed PCP with different adversary power levels

		Total	Successful	Unsuccessful	Failed
Simple adversary	Static-PCS	11	0	7	4
	SDN-PCS	8	8	0	0
Medium adversary	Static-PCS	11	0	8	3
	SDN-PCS	6	6	0	0
Advanced adversary	Static-PCS	12	1	10	1
	SDN-PCS	8	8	0	0

the number of required vehicles (γ) and the strategy timeout (δ) are initialized with default values and updated within simulations. We compare our proposed strategy to a Static PCS: a typical PCS that sums up all the existing PCSs where security parameters are static such as mix-context [13] and Rep [15]. We also consider three levels of adversary power: simple (λ= $0.4s^{-1}$), medium (λ=$0.5s^{-1}$) and advanced (λ=$0.6s^{-1}$).

Table II shows the number of the performed PCPs for each adversary level using the static PCS and the SDN-PCS. PCPs can be classified according to their results into three cases: (i) Successful: in this case the PCP runs after an optimal timeout and the number of vehicles which have privacy level under the threshold of privacy is equal to γ; (ii) Unsuccessful: While the PCP is performed, the number of vehicles that have a privacy level under the threshold is higher than γ; these vehicles will not be included in the PCP if the security parameters are not adequately adjusted; and finally (iii) Failed: in this case the PCP is not preformed because the number of required vehicles that are under the threshold is less than γ after the timeout. In total, the number of performed PCPs in the case of the static PCS is higher than the SDN-PCS. Our approach optimizes the number of PCPs to be executed .i.e the PCP is initiated only if it necessary. The SDN-PCS achieves 100 % successful PCSs. Indeed, the SDN-PCS adjusts the security parameters dynamically according to the vehicles context before each process. However, in the static PCS almost 0% of PCPs are successfully executed. The rest PCPs are either are unsuccessful (between 64% and 73%) or failed (between 8% and 36%). This is due to that fact that static PCS keep the security parameters unchanged whatever the PCS process is.

Figure 3a and Figure 3b show respectively the variation of the number of required vehicles (γ) and the strategy timeout (δ) over time in function of the adversary power. In contrast to static-PCS, PCS-SDN automatically adjusts these security parameters before each PCP.

For instance, SDN-PCS increases the number of required vehicles to perform the PCP when the adversary is powerful to increase his confusion. However, when the adversary is weaker, fewer vehicles are required to perform PCS and hence SDN-PCS decreases the strategy timeout to provide optimal response time. The strategy timeout results (Figure 3b) confirm the efficient tuning performed by SDN-PCS. Weaker is the adversary, longer is the PCP expiration time. Static-PCS keeps the same PCS parameters values despite the change of the vehicle context. These dynamic configurations of PCS security have positive impacts on the response time. This latter is defined by the delay between the triggering of the PCS and the time when the pseudonym is effectively changed. As illustrated in Figure 3c, the average of response time is improved for more than 38% when using SDN-PCS.

In addition, we evaluate the evolution of the privacy levels of vehicles over time. To this end, we use the anonymity set size as the privacy metric. The anonymity set size is defined as the number of vehicles that have participated in the PCP (γ). The privacy level of a vehicle v_i will then increase by (γ) each time it participates in the PCP. Figure 4 plots the overall privacy level which is calculated based on the average of all privacy levels of vehicles over time. For both Static PCS and SDN-PCS, the average levels of privacy remain above the threshold. It is worth mentioning that the overall average of privacy levels of vehicles using SDN-PCS is higher than one provided by static PCS.

TABLE III: PCS overhead: SDN-PCS vs static-PCS

	Static PCS	SDN-PCS
Simple adversary	200	91
Medium adversary	220	70
Advanced adversary	292	112

We evaluate in Table III the overhead in terms of number of messages needed to accomplish the PCS using SDN-PCS and Static PCS. It is obvious that our approach causes less overhead. Indeed more that 54% of messages are saved. The reason of this that SDN-PCS sends pseudonym changing requests only if needed.

VI. CONCLUSION

This paper proposes a privacy-preserving location scheme, called SDN-PCS, in which connected vehicles assisted by SDN controllers, decide whether and when to change their pseudonyms based on their context (density of the network, vehicle privacy level, attacker power, etc.). To the best of our knowledge, this is the first work to address the problem of location privacy using SDN paradigm. Extensive simulation results show that SDN-PCS provides less frequent pseudonym changes while better preserving the vehicle location privacy with less overhead compared to the state of the art solutions.

ACKNOWLEDGMENT

This work was supported by the H2020 5G-DRIVE project (ID: 814956), and the CONTACT project, CORE/SWISS/15/IS/10487418.

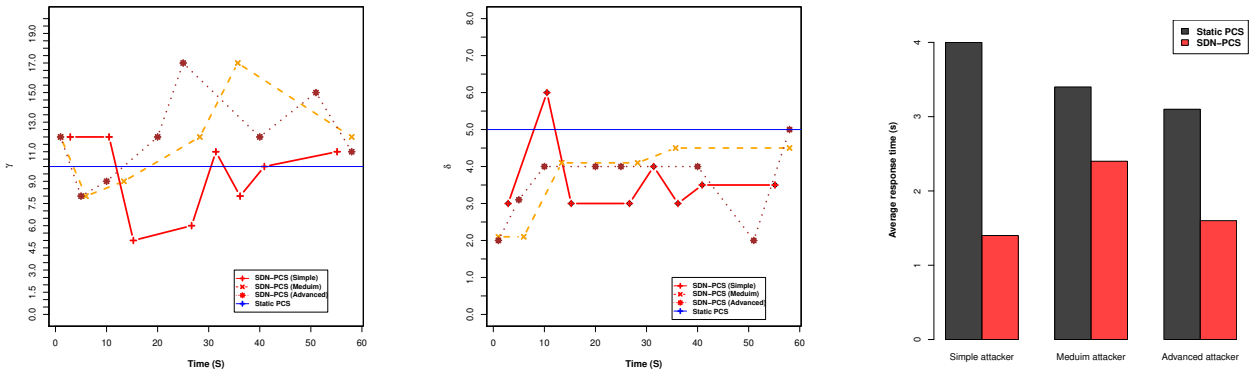
REFERENCES

[1] D. Eckhoff and C. Sommer, "Driving for big data? privacy concerns in vehicular networking," *IEEE Security and Privacy*, vol. 12, no. 1, pp. 77–79, February 2014.

[2] F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, and L. Wischhof, "Research challenges in intervehicular communication: lessons of the 2010 dagstuhl seminar," *IEEE Communications Magazine*, vol. 49, no. 5, pp. 158–164, 2011.

[3] ETSI, "Intelligent transport systems (ITS); security; pre-standardization study on pseudonym change management," *Standard, TC ITS*, 2018, technical report, ETSI.

[4] IEEE, "Ieee standard for wireless access in vehicular environments security services for applications and management messages," *IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006)*, pp. 1–289, April 2013.

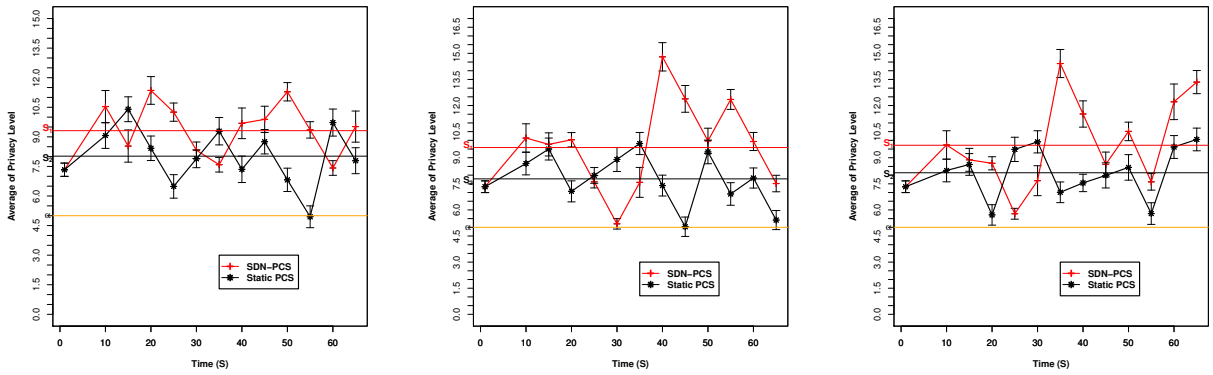


(a) The variation of of the number of required vehicles (γ).

(b) The variation of the strategy timeout (δ).

(c) Average of response time.

Fig. 3: Security parameters update and response time.



(a) Simple adversary.

(b) Medium adversary.

(c) Advanced adversary.

Fig. 4: The average of privacy levels of vehicles over time.

[5] ETSI, "Intelligent transport systems (its); security; trust and privacy management," *Standard, TC ITS*, 2018, technical specification, ETSI.

[6] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2017.

[7] X. Ge, Z. Li, and S. Li, "5g software defined vehicular networks," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 87–93, 2017.

[8] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proceedings of the First International Workshop on Wireless Networking for Intelligent Transportation Systems (Win-ITS)*, 2007.

[9] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, Jan 2012.

[10] A. Boualouache and S. Moussaoui, "S2si: A practical pseudonym changing strategy for location privacy in VANETs," in *Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on*, June 2014, pp. 70–75.

[11] ——, "Urban pseudonym changing strategy for location privacy in VANETs," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 24, no. 1-2, pp. 49–64, 2017.

[12] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "VLPZ: The vehicular location privacy zone," in *The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)*.

[13] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms-ideal and real," in *65th Vehicular Technology Conference*. IEEE, 2007, pp. 2521–2525.

[14] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in VANETs," in *10th International Symposium on Pervasive Systems, Algorithms, and Networks*. IEEE, 2009, pp. 648–652.

[15] A. Wasef and X. Shen, "Rep: Location privacy for VANETs using random encryption periods," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 172–185, 2010.

[16] A. Boualouache and S. Moussaoui, "TAPCS: Traffic-aware pseudonym changing strategy for vanets," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 1008–1020, 2017.

[17] X. Huang, R. Yu, J. Kang, N. Wang, S. Maharjan, and Y. Zhang, "Software defined networking with pseudonym systems for secure vehicular clouds," *IEEE Access*, vol. 4, pp. 3522–3534, 2016.

[18] X. Huang, J. Kang, R. Yu, M. Wu, Y. Zhang, and S. Gjessing, "A hierarchical pseudonyms management approach for software-defined vehicular networks," in *the 83rd IEEE Vehicular Technology Conference*, 2016.

[19] A. Alioua, S.-M. Senouci, S. Moussaoui, H. Sedjelmaci, and A. Boualouache, "Software-defined heterogeneous vehicular networks: Taxonomy and architecture," in *2017 Global Information Infrastructure and Networking Symposium (GIIS)*. IEEE, 2017, pp. 50–55.

[20] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "Non-cooperative location privacy," *Dependable and Secure Computing, IEEE Transactions on*, vol. 10, no. 2, pp. 84–98, 2013.

[21] S. H. Bouk, G. Kim, S. H. Ahmed, and D. Kim, "Hybrid adaptive beaconing in vehicular ad hoc networks: a survey," *International Journal of Distributed Sensor Networks*, vol. 11, no. 5, p. 390360, 2015.

[22] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved ivc analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, Jan 2011.

[23] SUMO, "Simulation of urban mobility," http://sumo.sourceforge.net/, 2019.