Software-Defined Location Privacy Protection for Vehicular Networks

Abdelwahab Boualouache, Ridha Soua, Qiang Tang and Thomas Engel

Abstract While the adoption of connected vehicles is growing, security and privacy concerns are still the key barriers raised by society. These concerns mandate automakers and standardization groups to propose convenient solutions for privacy preservation. One of the main proposed solutions is the use of Pseudonym-Changing Strategies (PCSs). However, ETSI has recently published a technical report which highlights the absence of standardized and efficient PCSs [1]. This alarming situation mandates an innovative shift in the way that the privacy of end-users is protected during their journey. Software Defined Networking (SDN) is emerging as a key 5G enabler to manage the network in a dynamic manner. SDN-enabled wireless networks are opening up new programmable and highly-flexible privacy-aware solutions. We exploit this paradigm to propose an innovative software-defined location privacy architecture for vehicular networks. The proposed architecture is context-aware, programmable, extensible, and able to encompass all existing and future pseudonym-changing strategies. To demonstrate the merit of our architecture, we consider a case study that involves four pseudonym-changing strategies, which we deploy over our architecture and compare with their static implementations. We also detail how the SDN controller dynamically switches between the strategies according to the context.

Abdelwahab Boualouache
SnT, University of Luxembourg, Esch-sur-Alzette, AVE, 4365, Luxembourg, e-mail: abdelwahab.boualouache@uni.lu

Ridha Soua
SnT, University of Luxembourg, Esch-sur-Alzette, AVE, 4365, Luxembourg, e-mail: ridha.soua@uni.lu

Qiang Tang
Luxembourg Institute of Science and Technology (LIST), e-mail: qiang.tang@list.lu

Thomas Engel
SnT, University of Luxembourg, Esch-sur-Alzette, AVE, 4365, Luxembourg e-mail: thomas.engel@uni.lu

1 Introduction

As part of the vision of 5G, connected vehicles will be an important pillar of Cooperative Intelligent Transportation Systems (C-ITS), with the aim to ensure road safety, avoid traffic congestion and provide a better driving experience for users during their journey. Although the deployment stage for connected vehicles is imminent, many security and privacy issues are still unsolved. Location privacy is one of the main issues that may impede the wide acceptance of Cooperative Connected and Automated Mobility (CCAM) applications. Indeed, location tracking of vehicles may reveal every place visited by drivers. This is because there is generally a one-to-one relationship between the vehicle and its driver. The visited locations may include very personal places like hospitals, banks, insurance companies, etc. and hence can reveal sensitive information about the end-user.

On the other hand, the main wireless communication technologies for connected vehicles, such as IEEE802.11p, present several privacy concerns. Indeed, IEEE802.11p mandates that each connected vehicle should frequently send a safety message, called CAM (Cooperative Awareness Message), to ensure cooperative awareness among neighboring vehicles. These messages include sensitive information such as identifiers, positions, speeds, etc, and are sent in clear text; hence vehicles could be tracked on the basis of the information transmitted by the Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. To mitigate this privacy risk, the use of pseudonym schemes has received significant interest from the research community and standardization authorities. For instance, both the European standard ETSI TS 102 941 [1] and the American standard SAE J2735 [2] have adopted a pseudonym scheme. However, several studies have shown that the use of a simple pseudonym-changing is insufficient to provide unlinkability between the pseudonyms and have suggested using strategies for changing the pseudonyms. Although, there is a significant number of proposed Pseudonym-Changing Strategies (PCSs), there are no recommendations by standardization bodies for PCSs to apply. The main reasons for this can be summarized as follows: (i) several proposed strategies are strongly topology-dependent i.e. they could only be applied in a given situation or area such as signalized intersections, parking lots, and gas stations; (ii) some strategies propose the use of radio silence without considering its critical impact on the exchange of safety messages, or dynamically readjusting radio silence duration; (iii) each PCS is evaluated with individual privacy metrics that may not be suitable for another PCS. This absence of unified evaluation metrics complicates the comparison between existing strategies; (iv) The scarcity of scientific studies focusing on the non-cooperation behavior of vehicles. Selfish vehicles could significantly decrease the efficiency of PCSs; (v) most of the existing PCSs assume a strong global passive adversary. However, this assumption is not realistic, since the global presence of the adversary is difficult to achieve due to the large scale of deployment of connected vehicles, and the high cost of ensuring complete coverage; and (vi) pseudonyms could be easily used to perform Sybil attacks. This vulnerability is not taken into the account by most of the strategies proposed in the literature.

One possible solution for dealing with these various PCSs is to propose a comprehensive architecture that is able to encompass all of them and their intrinsic features. This architecture should be forward-looking in the sense that it should support future PCS solutions. Software-Defined Networking (SDN) has recently been exploited to provide a dynamic and context-aware security solution for vehicular networks [3]. In this chapter, we exploit SDN to propose a software-defined architecture for location privacy in vehicular networks. This architecture extends and leverages the concepts of SDN to PCSs and ensures the selection of the appropriate PCS according to the context of vehicles and other factors, as will be detailed later. The SDN control plane orchestrates the selection and adjusts the parameters of the selected strategy dynamically, based on information received from the data plane. The SDN strategy rules are also forwarded from the control plane to the data plane to ensure the correct execution of the selected PCS. The proposed architecture is flexible and enables the efficient integration of new proposed solutions and new functions of the PCS. The contributions of this work can be summarized as follows:

- Integration of SDN into vehicular networks, allowing new PCSs to be deployed, easily updated and dynamically reconfigured.
- Introduction of novel pseudonym-changing modules in the control plane and the definition of their different interactions to ensure a context-aware PCS.
- Introduction of novel complementary pseudonym-changing modules in the data plane and the definition of their interactions.
- Definition of SDN rules (which can be modified dynamically at the controller) to establish a set of actions that will handle the PCS.
- Definition of a Sybil attack agent to interact with the external misbehavior system controller.
- Definition of self-learning module that is able to analyze and learn from its immediate context while autonomously adapting the PCS accordingly to ensure a high level of privacy protection. This module is crucial, as it guarantees network intelligence and leads to a network that is self-privacy-preserving.

2 Pseudonym-Changing Strategies: Standardization Efforts and Open Issues

Security standardization bodies have agreed to adopt PCS to protect the location privacy of connected vehicles. However, while in the US, the Society of Automotive Engineers (SAE) suggests that vehicles change their pseudonym every five minutes [2], the European telecommunications standardization organization, ETSI, does not suggest the adoption of any PCS [1]. In the light of this, many PCSs are proposed in the literature. In [4], we presented a comprehensive survey and classification of these strategies. This paper also highlights open issues and presents recommendations, including the importance of developing a dynamic system to select the applying PCS according to the vehicular context. Recently, ETSI published a technical report

(ETSI TR 103 415) [1] that presents a pre-standardization study of PCS. This document surveys the existing categories of strategies. It also discusses and describes the suggestions of the European projects (PRESERVE, SCOOP@F, and C2C-CC) regarding PCS. The document identifies the open issues of PCSs and proposes a set of recommendations addressing these issues. In the following, we discuss the open issues highlighted in [1, 4] and the related recent advances

- **Impact on road safety**: as shown in [4], strategies using radio silence are the most efficient solutions. However, their major drawback is their significant negative impact on safety-related applications. This was first investigated in [5], where the authors recommend that the silent period should be shorter than two seconds and that long silent periods can result in hazardous situations, since many safety messages will not be transmitted due to radio silence. The ETSI technical report [1] also discusses the problems of “missing vehicles" and “guest vehicles". Missing vehicles are those that put radio silence into effect after changing their pseudonyms; at the end of this period, these vehicles suddenly appear in the LDMs (Local Dynamic Map) of neighboring vehicles. This may generate unpredictable reactions as highlighted in [1]. In contrast, the problem of the guest vehicle is observed when a vehicle changes its pseudonym while his old pseudonym still populates the LDMs of its neighboring vehicles [6]. Subsequently, LDM messages contain two entries that correspond to the same vehicle, leading to a misinterpretation of the surrounding environment by neighboring vehicles. Unlike the missing vehicle problem, the ghost vehicle problem is not only linked to radio silence based strategies, but to PCSs in general.
- **Non-cooperative behavior**: by triggering the change of their pseudonyms at the same time slot, cooperative vehicles ensure a high level of anonymity and create confusion for the attacker. Consequently, the existence of non-cooperative vehicles will significantly hinder the efficiency of the PCS specifically under lower vehicular density. The authors of [7] study PCSs under a non-cooperative environment. They propose a game theory model and find a Nash equilibrium of the PCS under different types of games (static/dynamic, with and without complete information). Other works such as [8] and [9] propose incentive mechanisms to motivate non-cooperative vehicles to participate in the PCS.
- **Attacker model:** It is not trivial to estimate the power of tracking attackers that may exist in the future deployment of vehicular networks. Attacker power can be expressed in terms of tracking capabilities (strong or weak sniffing stations, efficiency of the tracking algorithm, etc.) and the coverage area. In addition, it is critical to properly define a realistic attacker model. For this reason, most of proposed PCSs have assumed the extreme case of the attacker model (global attacker full of capabilities); however, this assumption is not realistic, because global coverage entails a significant surveillance cost. Consequently, the authors of [10] propose a mid-sized attacker whose power is in between that a local attacker and a global one. They also distinguish three tracking periods (i.e short-term, mid-term, and long-term) and two levels of surveillance granularity (i.e Road-level and Zone-level).

- **Evaluation metrics:** many metrics are proposed to assess the performance of PCSs. The recent study carried out by Zhao et al. [11] show that there is no single privacy metric that outperforms all others under different contexts (mobility, traffic conditions, road section, etc.). For this reason, it is recommended to combine all metrics to obtain a fair performance evaluation of a PCS.
- **Privacy model:** the privacy level depends mainly on the considered attacker model and the evaluation metrics. The authors of [7] proposed a linear model to quantify the loss of privacy after the last change of pseudonym. In this model, the privacy level of vehicles linearly decreases according to a sensitivity parameter, which characterizes the power of the adversary. However, this model has two major drawbacks: (i) it does not specify how the sensitivity parameter is measured. (ii) the linearity of this model is not justified.
- **Sybil attacks:** In this attack, vehicles use multiple identities, called Sybils, which can be exploited to create a fake traffic jam and hence to alter other vehicles' perceptions. Pseudonyms could be exploited to launch Sybil attacks. The ETSI technical report [1] gives some recommendations on thwarting Sybil attacks, such as setting the maximum number of pseudonyms that can be used simultaneously and the minimum duration for which the pseudonyms should be used. The technical report also recommends the use of misbehavior detection systems.
- **Pseudonym lock:** ETSI standards specify that the PCS could be locked on-demand for a maximum of 255s, in particular when a critical safety situation occurs. The priority levels of such a situation are respectively “0" or “1" [12]. PCS locking is also proposed by the SAE. However, the conditions when the pseudonyms are locked are not yet defined.
- **Pseudonym reuse:** Although the reuse of pseudonyms minimizes the storage capacity and facilitates the management of pseudonyms, it can decrease the level of privacy. This is why the reuse of pseudonyms is not recommended as a privacy best practice. However, the Car2car consortium considers the reuse of pseudonym while defining some KPI to increase the privacy level [4].

3 Proposed Architecture: Building blocks

Our self-privacy-preserving architecture leverages the SDN paradigm and thus follows its main principle, which is the separation between the data and the control plane. The control plane is responsible for dynamically selecting the PCS, adjusting the parameters of strategy, and planning the strategy rules. On the other hand, the data plane translates the defined rules into actions to apply the PCS. The communications between the control plane and the data plane are secure.

3.1 Control Plane

Figure 1 shows the logical modules of the control plane in our architecture. The PCS module receives a demand from the application layer to provide the location privacy service. This module chooses the most convenient PCS to be executed based on the information received from two modules: the Mobility and Topology module and Attacker Model module. Once the strategy is selected, the PCS module invokes (i) the Parameter Settings module to request the parameters of the strategy; (ii) the Incentive Model module to request the appropriate incentive method to motivate non-cooperative vehicles; and (iii) the Privacy Metric module to request indicators and KPIs for the evaluation of PCS performance. In the following, we detail these modules.

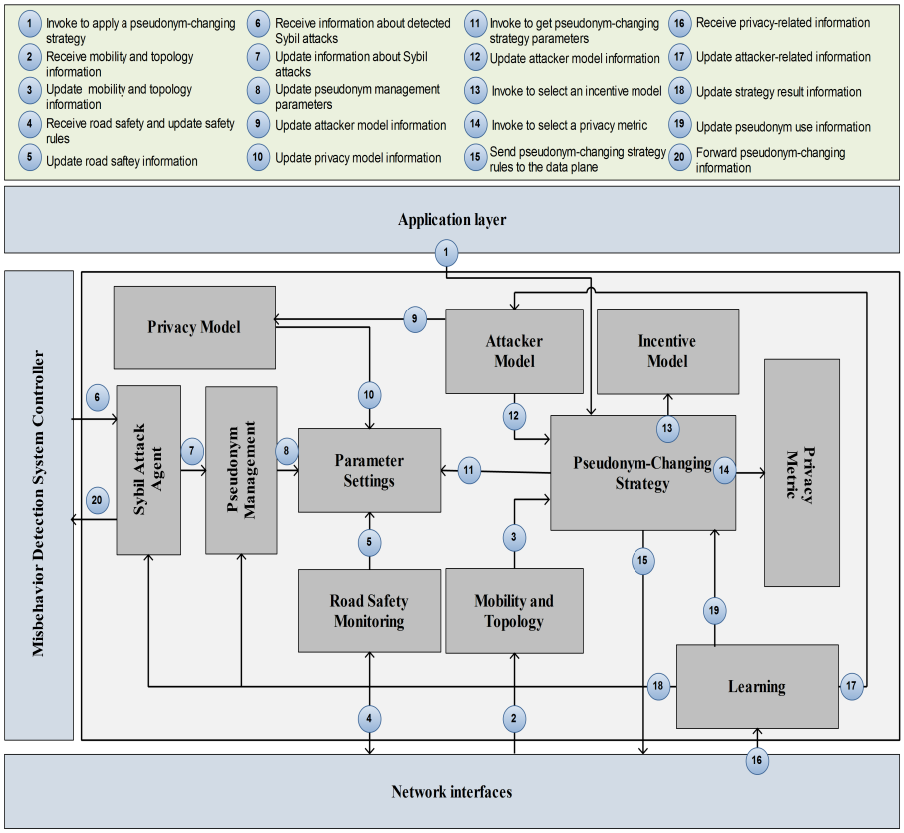

Fig. 1 The logical modules of the control plane and the interactions between them.

- **Road Safety Monitoring:** this module monitors road conditions and its impact on traffic safety. Based on this assessment, the module develops appropriate SDN rules which are sent to the data plane. In addition, this module provides the necessary information to the Parameter Settings module to tune the PCS parameters, such as the duration of radio silence and the lock period.
- **Misbehavior Detection System Controller:** this is an external component, which detects misbehaving attacks such as message injection, denial of service (DoS) and Sybil attacks. The SDN controller of our self-privacy-preserving architecture uses the information received from the Misbehavior Detection System Controller to update its parameters in order to limit Sybil attacks and returns information to help in detecting Sybil attacks and accurately evaluating the trust levels of vehicles.
- **Sybil Attack Agent:** this interface is used to interact with the Misbehavior Detection System Controller, receiving information from it and forwarding it to the Pseudonym Management module to adjust some PCS parameters. It also receives information from the Learning module and forwards this to the Misbehavior Detection System Controller to enhance the attack detection ratio.
- **Pseudonym Management:** this module plans the rules that orchestrate the use of pseudonyms: the reuse of pseudonyms, the frequency of changing of pseudonyms, the number of pseudonyms that can be used in parallel, etc. This module receives information from both the Sybil Attack Agent and learning modules and sends the resulting rules to the Parameter Settings module.
- **Privacy Model:** This is used to model the loss of privacy of vehicles over time. As explained in the previous section, the loss of privacy mainly depends on the strength of the attacker model. For this reason, this module receives input from the Attacker Model module. The Privacy Model provides input to the Parameter Settings module, which in return specifies the parameters of the Privacy Model.
- **Mobility and Topology:** this module monitors the mobility pattern of vehicles and the road topology in real time.
- **Parameter Settings:** this module sets the different parameters of the PCS, such as the duration of the radio silence period and the minimum duration of the use of pseudonyms. The definition of these parameters is made according to the information received from the Road Safety, Pseudonym Management, and the Privacy Model modules.
- **Attacker Model:** this module evaluates the power of the attacker. As discussed in the previous section, the attacker can be internal or external, local or mid-sized, long-term. It can perform simple syntactic linking of pseudonyms, but can also carry out more advanced semantic linking of pseudonyms. This module gets regular updates from the learning model and sends feedback to the Pseudonym-Changing Strategy module.
- **Incentive Model:** this module defines the incentive model, which is used to motivate selfish vehicles to participate in the PCS.
- **Privacy Metric:** this module defines the privacy metrics used to evaluate the PCS. It worth mentioning that the privacy metrics can be selected by the PCS to evaluate its own performance.

- **PCS Module:** this module defines the strategy to be executed based on the information received from the Mobility and Topology module and the Attacker Model module. Once the strategy is selected, this module invokes the Parameter Settings module to obtain the most appropriate parameters of the selected strategy. This module also invokes the Privacy Metric module and the Incentive Model module to select the evaluation metric and the incentive method respectively.
- **Learning:** this module periodically receives privacy-related information from the data plane (i.e the privacy levels of vehicles, the presence of an attacker, and the set of selfish vehicles). This information is analyzed and forwarded to the corresponding modules: (i) the Attacker Model module to adjust the attacker model being used; (ii) the PCS module to tune the strategy parameters, and the Incentive Model module, and to select an additional potential privacy metric. (ii) the Pseudonym Management module to adjust pseudonym management related parameters, and finally (iv) the Sybil Attack Agent, which forwards pseudonym-changing information to the Misbehavior Detection System Controller. The purpose is to support this controller in the accurate detection of Sybil attacks and trust assessment of vehicles.

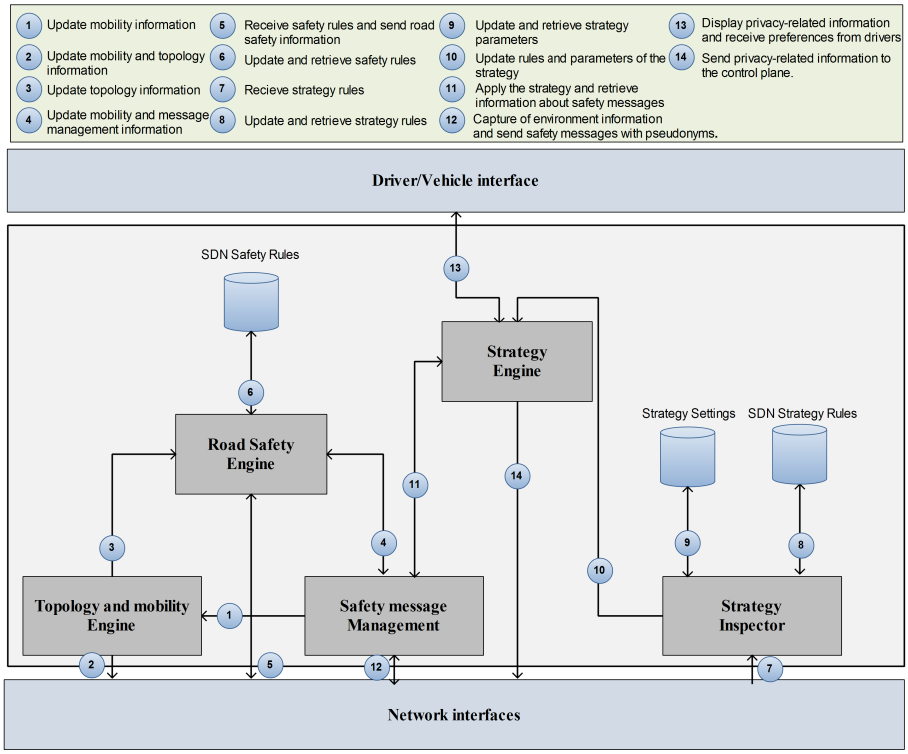

Fig. 2 The logical components of the data plane and the interactions between them.

3.2 Data Plane

The data plane is composed of the different vehicles that are involved in the PCS. Figure 2 depicts the modules of the data plane, which are responsible of the execution of the PCS. The data plane uses the vehicles' communication interfaces to collect pertinent information concerns the surrounding vehicular environment. The data plane sends mobility, safety, and privacy information to the control plane, while it receives safety and strategy rules. In the following, we describe the modules and the databases of the data plane:

- **Safety Message Management:** this module sends and receives pseudonymous safety messages. It also receives instructions from the Strategy Engine. These instructions vary according to the applied strategy. In addition, this module provides the status of the surrounding environment and the impact of the applied PCS to the Road Safety Engine, the Topology and the Mobility engine, and finally to the Strategy Engine.
- **Mobility and Topology Engine:** Equipped with a map and GPS, this module sends the mobility information of the vehicle such as position, speed, and acceleration and the topology information to the Road Safety Engine and to the control plane.
- **SDN Safety Rules:** This is a database, which contains the safety rules that are used to assess road conditions. The rules data is received from the control plane.
- **Road Safety Engine:** this module receives, stores and updates the safety rules received from the control plane. These rules are used to evaluate road safety based on the information received from the Topology and Mobility Engine and the Safety Message Management module. This module periodically sends road safety information to the control plane.
- **SDN Strategy Rules:** This is a database that contains the rules related to PCS. These rules describe where, when and how pseudonyms change. The database is regularly updated by the Strategy Inspector module; based on the information received from the control plane.
- **Strategy Settings:** This is a database that contains the settings of the applied strategy such as the duration of radio silence period after the changing of pseudonym. This database is also regularly updated by the Strategy Inspector module according to the information received from the control plane.
- **Strategy Inspector:** this module represents an interface, which communicates with the PCS module of the control plane. It receives information from the SDN controller(s) and stores them in two databases: the SDN Strategy rules and the Strategy Settings databases. This module also forwards these PCS rules and settings to the Strategy Engine module.
- **Strategy Engine:** this module executes the PCS according to the rules and settings received from the Strategy Inspector module. To execute the strategy, the module continuously monitors and sends instructions to the Safety Message Management module. This module provides privacy protection related information to the driver

from whom it receives privacy level recommendations. This module also sends privacy-related information to the control plane.

4 Case Study

To demonstrate the merit of our proposed architecture, we conducted the following case study. As shown in Figure 3 (1), we populated a Software-Defined Location Privacy Controller (SDLP) with four state-of-the-art PCSs: UPCS [13], TAPCS [14], PRIVANET [9] and SocialSpots [15]. In this section, we first show how these strategies are integrated into our architecture. Then, we illustrate how the SDLP performs a context-aware PCS selection. The context is mainly defined by mobility and topology, as well as the attacker model. Finally, we conduct a simulation-based study to demonstrate how our proposed architecture dynamically updates the security parameters of each strategy.

4.1 PCSs Deployment

Table 1 The deployments of PCSs in the self-privacy-preserving architecture

	Mobility and topology	**Parameter setting**	**Attacker model**	**Privacy model**	**Privacy metric**	**Incentive model**
UPCS [13]	Signalized intersection	Red traffic light duration: 30s, 60s	Global external passive and local internal passive (Semantic and syntactic linking)	No	The entropy of the annonymity set	No
SocialSpots [15]	Signalized intersection	Red traffic light turns green	Global external passive (Syntactic linking)	No	The size of the anonymity set	Yes
TAPCS [14]	Traffic congestion	Speed threshold	Global external passive and local internal passive (Semantic and syntactic linking)	No	The entropy of the anonymity set	No
PRIVANET [9]	Roadside Infrastructure e.g. Gas station	The capacity of RI The threshold of privacy	Global external passive and local internal passive (Semantic and syntactic linking)	Yes	The size of the anonymity set	Yes

Our proposed architecture is flexible enough to support any state-of-the-art PCS. Table 1 shows how the considered strategies are mapped to our architecture. This table has six columns: (i) Mobility and topology: specifies the topology where the strategy can be used; (ii) Parameter Setting: specifies the parameters of the strategy; (iii) Attacker model: specifies that attacker model from which the strategy provides protection; (iv) Privacy model: specifies if the strategy uses a privacy model or not; (v) Privacy metric: specifies the metric used to evaluate the strategy; (vi) Incentive model: specifies if the strategy uses an incentive model or not.

Control plane modules are activated or deactivated according to the requirements of each PCS. For example, the Incentive Model module is disabled for UPCS and TAPCS since these strategies do not propose any mechanism to motivate non-cooperative vehicles to change their pseudonyms; while the Privacy Model module is only activated for PRIVANET strategy.

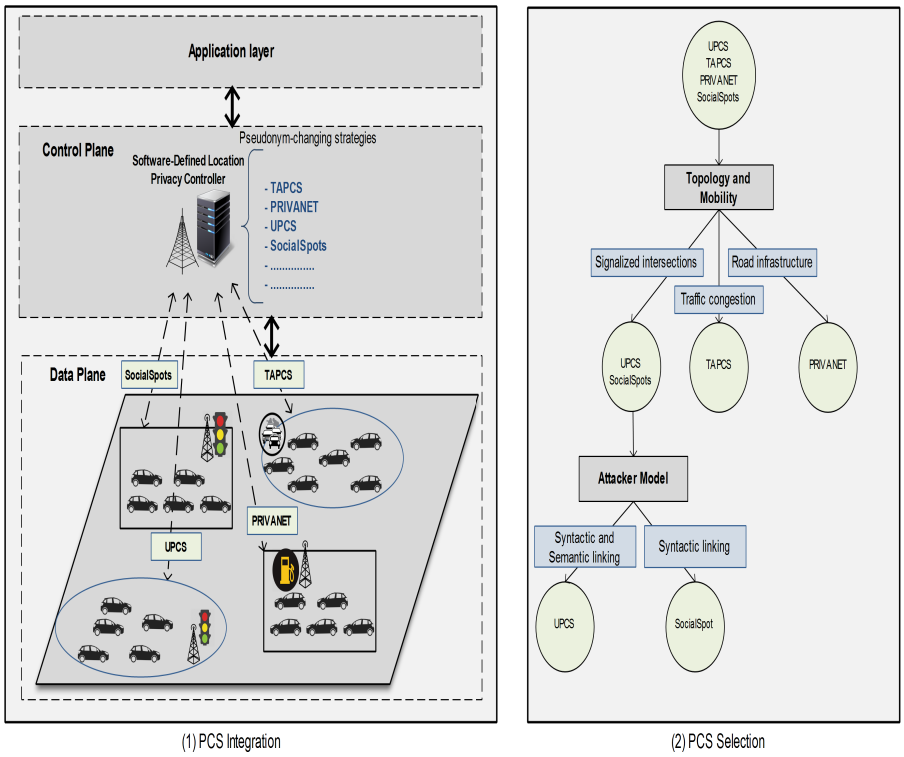

Fig. 3 The selection of pseudonym changing strategy

Figure 3 (2) illustrates the different steps of the selection of a PCS. The SDLP first checks the information received from the Mobility and Topology module. For instance, if the vehicle is entering a signalized intersection, two PCSs could be applied to this context: UPCS and SocialSpots. To decide which of the two strategies to apply, SDLP checks information received from the Attacker Model module. If the attacker model can perform both syntactic and semantic pseudonym linking attacks, then UPCS is selected. Otherwise, if the attacker can perform only syntactic attacks, SocialSpots is selected. More details on syntactic and semantic pseudonym linking attacks can be found in [4].

4.2 Simulation Setup

We carried out a simulation-based analysis to demonstrate the merit of our SDN-based and self-learning architecture and how it dynamically adapts the PCS security parameters to the context. This simulation-based analysis was performed using Veins

Table 2 The configuration of pseudonym-changing strategies

Strategy	Changed context	Configuration	Action	Results
SDN-based UPCS [13]	Road safety	10% of vehicles in dangerous situation	Pseudonym lock	Low safety risk Acceptable privacy level
		20% of vehicles are in dangerous situation	Pseudonym lock	Low safety risk. Acceptable privacy level
SDN-based TAPCS [14]	Attacker model	Simple attacker	Select privacy metric	The size of the anonymity set
		Medium attacker	Change the privacy metric	The entropy of the anonymity set
		Advanced attacker	Keep the privacy metric	The entropy of the anonymity set
SDN-based PRIVANET [9]	Privacy model	Sensitivity parameter = 0.1	Update privacy model	High privacy level
		Sensitivity parameter = 0.2	Update privacy model	Low privacy level

Simulation Framework [16]. The considered scenario is similar to that proposed in [9]. Three strategies are simulated: UPCS, TAPCS, and PRIVANET. SocialSpots was excluded, as it has the same application context (signalized intersections) as UPCS.

Table 2 details the configurations of the simulated strategies. This table has four columns: (i) Changed context: specifies the context we change during the simulation; (ii) Configuration: specifies the values we assign to the context' parameters; (iii) Action: specifies the action to perform when the parameter is changed; (iv) Results: specifies the obtained results when the action is applied. To demonstrate the dynamic changing of PCS parameters according to context, three different scenarios are considered.

1. **Scenario 1**: uses UPCS strategy in a road safety context, where the number of vehicles in a dangerous situation can be 10% or 20%. The pseudonym changing in such a situation can generate traffic collisions and accidents.
2. **Scenario 2**: uses TAPCS strategy, where we study how this strategy adapts the privacy metric to the attacker model. Three configurations of the attacker model are considered: simple, medium, and advanced.
3. **Scenario 3**: uses PRIVANET focusing on the privacy model. We consider two configurations of this model by varying the sensitivity parameter value, which characterizes the power of the adversary.

4.3 Simulation Results

Figure 4 compares the static implementation UPCS (static UPCS) to its SDN-based variant (SDN-based UPCS). Two performance indicators are considered: the privacy level and safety. As shown in Figure 4, static UPCS provides a higher level of privacy protection compared to SDN-based UPCS. However, SDN-based UPCS has a lower safety risk than static UPCS. The reason for this, as described in Table 2, is that SDLP takes an action to lock pseudonym-changing processes of vehicles in a dangerous situation. This lock slightly decreases the privacy protection level, while reducing the safety risk.

Figure 5 makes a comparison between Static TAPCS and SDN-based TAPCS. In Static TAPCS, the entropy of anonymity set is used as a performance metric,

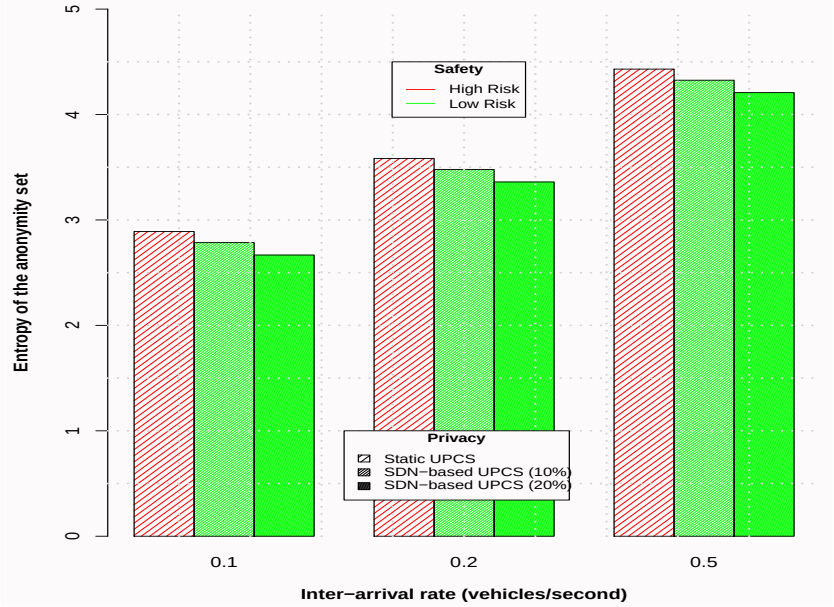

Fig. 4 Static UPCS vs SDN-based UPCS

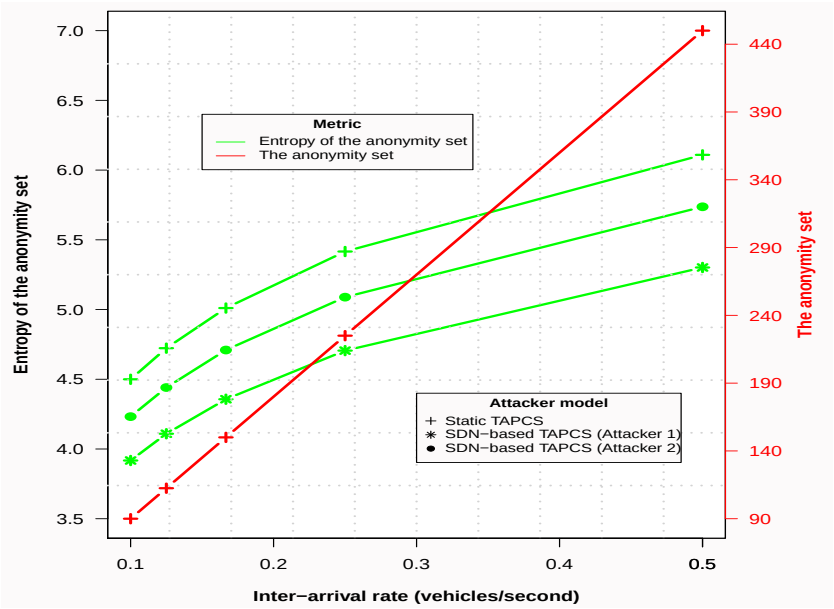

Fig. 5 Static TAPCS vs SDN-based TAPCS

whatever the used attacker model. However, the SDN-based TAPCS varies the performance metric according to the power of the attacker. For instance, the size of the anonymity set is chosen when the attacker is simple, while the entropy of the anonymity set is considered when the attacker is medium or advanced. This selection of the performance metrics is based on the probabilities of distinction between vehicles in the considered area. In the former case, these probabilities are equal and hence the measuring size of the anonymity set performs well. In the latter case, these probabilities are not equal; hence the need to take the entropy into account.

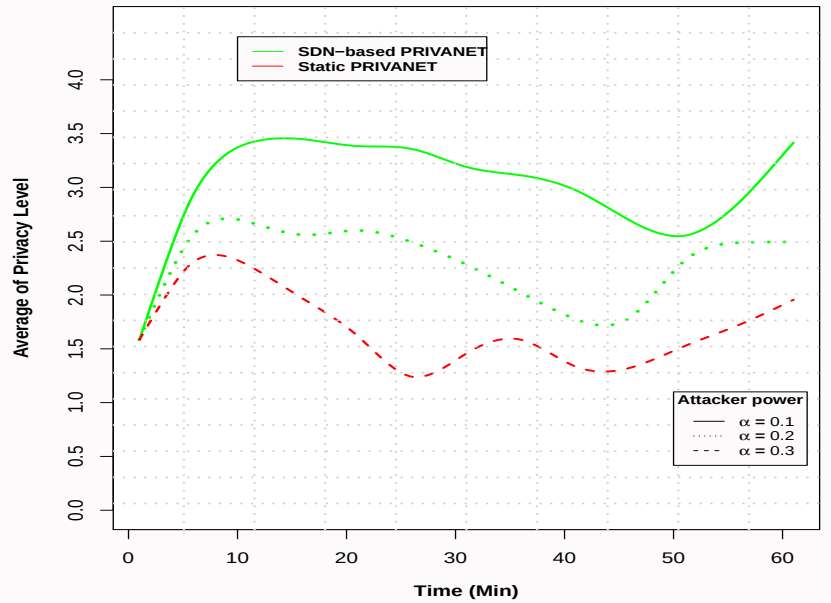

Fig. 6 Static PRIVANET vs. SDN-based PRIVANET

Finally, we compare the static implementation of PRIVANET and the SDN-based version. As illustrated in Figure 6, the sensitivity parameter (α), which characterizes the power of the attacker, remains unchanged in Static PRIVANET and is equal to 0.3. However, for SDN-based PRIVANET, the sensitivity parameter is updated according to the information received from the data plane. The change in the power of the attacker (the sensitivity parameter) has a direct impact on the privacy level obtained by vehicles. Indeed, as illustrated in Figure 6, the high values of the average of privacy are obtained when the sensitivity parameter equals 0.1. However, the lower values of the average of privacy are obtained when the sensitivity parameter equals 0.3.

5 Conclusion

The imminent deployment of connected vehicles requires significant attention to the security and privacy aspects. Privacy protection is a critical issue that influences the user acceptance of this technology. Pseudonym-changing strategies are considered as the key solution to overcome this acute need. However, the absence of recommended pseudonym-changing strategies (PCSs) represents an obstacle to achieving this objective. To this end, we propose an innovative architecture that exploits Software-Defined Networking (SDN), one of the key technologies for 5G networks. Our proposed architecture is flexible and self-learning and hence can encompass PCSs proposed so far in the literature and even upcoming PCSs. The selection of the appropriate PCS and it security settings are context-aware. The control plane is modular and includes the main building-blocks of PCSs which can support any future solution. As future work, we plan to carry out extensive simulations to assess the performance of the proposed architecture.

Acknowledgment

This work was supported by the 5G-DRIVE project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 814956. Also, this work is a part of the 5G-MOBIX project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825496. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains

References

1. ETSI TR 103 415, "Intelligent Transport Systems (ITS); security; pre-standardization study on pseudonym change management," *ETSI standards*, 2018.
2. J2945/1, "On-board system requirements for V2V safety communications," *SAE Standards*, 2016.
3. S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, "Sdn-based secure and privacy-preserving scheme for vehicular networks: A 5g perspective," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 8421–8434, 2019.
4. 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.
5. S. Lefevre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of v2x privacy strategies on intersection collision avoidance systems," in *Vehicular Networking Conference (VNC), 2013 IEEE*, Dec 2013, pp. 71–78.
6. I. B. Jemaa, A. Kaiser, and B. Lonc, "Study of the impact of pseudonym change mechanisms on vehicular safety," in *2017 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2017, pp. 259–262.

7. 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.
8. B. Ying, D. Makrakis, and Z. Hou, "Motivation for protecting selfish vehicles' location privacy in vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 64, no. 12, pp. 5631–5641, 2015.
9. A. Boualouache, S.-M. Senouci, and S. Moussaoui, "PRIVANET: An efficient pseudonym changing and management framework for vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, 2019.
10. J. Petit, D. Broekhuis, M. Feiri, and F. Kargl, "Connected vehicles: Surveillance threat and mitigation," *Black Hat Europe*, p. 11, 2015.
11. Y. Zhao and I. Wagner, "On the strength of privacy metrics for vehicular communication," *IEEE Transactions on Mobile Computing*, vol. 18, no. 2, pp. 390–403, 2018.
12. ETSI TS 101 539-1 (V1.1.1), "Intelligent Transport Systems (ITS); V2X applications; part 1:Road Hazard Signalling (RHS) application requirements specification," *ETSI standards*, 2013.
13. A. Boualouache and S. Moussaoui, "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.
14. ——, "TAPCS: Traffic-aware pseudonym changing strategy for VANETs," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 1008–1020, 2017.
15. 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, 2011.
16. 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.