PREXT: Privacy Extension for Veins VANET Simulator

Karim Emara
University of Luxembourg (SnT), Luxembourg, karim.emara@uni.lu
Faculty of Computer and Information Sciences, Ain Shams University, karim.emara@cis.asu.edu.eg

***Abstract*—Preserving location privacy is an important aspect in vehicular ad-hoc networks. In VANET, vehicles are continuously broadcasting and receiving spatiotemporal information to/from the surrounding vehicles to form 360 degrees of traffic awareness. This exchanged information can be collected reconstruct the vehicle trajectories, which threatens the driver's privacy. Although location privacy is thoroughly studied in the past decade, it is usually skipped in VANET simulators. In this paper, we propose a location privacy extension, PREXT, for Veins framework. Currently, PREXT supports seven privacy schemes of different approaches including silent period, context-based and mix-zone and can be easily extended to include more schemes. It includes adversary modules that can eavesdrop vehicle messages and track their movements. This adversary is used in measuring the gained privacy in terms of several popular metrics such as entropy, traceability and pseudonym usage statistics.**

***Index Terms*—Security and privacy; VANET simulation; Veins; OMNeT++**

I. Introduction

[1] Security and privacy are crucial aspects in vehicular adhoc networks (VANET). Vehicles must communicate in a secure and private way to be able to provide the prospective services without worrying about breaking the system or threating the driver privacy. One essential requirement for safety applications is to periodically broadcast beacon messages containing the spatiotemporal information of the vehicle. Basically, these messages are identified by periodically-changed pseudonyms and signed by a short-term private key assigned to the vehicle. Vehicles receiving these messages can verify the authenticity of the sending vehicle and the message integrity by checking the anonymous certificate attached with the message and the embedded signature, respectively. There is a consensus on this public key infrastructure to be used in VANET [2] illustrated in the current standardization bodies (ETSI TS 102 941 [3] and IEEE 1609.2 WG [4]).

However, using pseudonyms in beacons may yield to track vehicle movements even if they are periodically changed [5], [6]. The included spatiotemporal information in beacons allows correlating messages of old and new pseudonyms. If beacons are massively collected, vehicle traces can be reconstructed and imposing a serious privacy threat upon the drivers. Although the exchanged beacons contain no personal information, further inference attacks can be performed to de-anonymize the reconstructed traces [7], [8] and identify the driver's sensitive whereabouts.

There are several pseudonym change schemes (i.e., privacy schemes) that try to prevent continuous tracking of vehicles using a silence period before a pseudonym change or by changing pseudonyms in mix-zones where the vehicle trajectory is unpredictable. Although privacy in VANET is throughly studied in the past decade, there is only few VANET simulators that supports privacy aspects. Moreover, privacy schemes are usually evaluated using different assumptions and mobility models in terms of different privacy metrics. This inconsistent evaluation hardens identifying the actual performance of different privacy schemes.

In this paper, we propose a privacy extension, PREXT, for Veins framework [9] to facilitate evaluating and comparing privacy schemes. We choose Veins framework because it offers realistic models of IEEE 802.11p and IEEE 1609.4 DSRC/WAVE network layers along with the realistic vehicular mobility model provided by SUMO traffic simulator [10]. Thus, privacy schemes can be evaluated in a realistic VANET environment rather than over-simplified situations. Moreover, supporting privacy schemes inside a VANET simulator will encourage protocol designers to consider privacy constraints while designing and evaluating network and application protocols. In addition, the impact of privacy schemes on application functionalities, especially safety applications, is sporadically evaluated. The proposed privacy extension will facilitate evaluating the privacy impact whether on communication protocols or different applications.

The rest of this paper is organized as follows. In Section II, we review VANET simulators including those support privacy and security aspects. The architecture of PREXT is presented in Section III. In Section IV, we explain the adversary modules that evaluates privacy schemes and calculates various privacy metrics. In Section V, we discuss the provided metrics and statistics. Last but not least, the evaluation of PREXT performance along with a comparison between privacy schemes are discussed in Section VI.

II. Related Work

There are several simulation tools for VANET such TraNs [11], VANET MobiSim [12], Veins [9] and iTETRIS [13]. Although VANET is a special type of MANET, MANET simulators cannot be directly used for VANET unless the vehicular

[1] This work is done while the author affiliated with the Technical University of Munich (TUM), Germany. This paper is an extended version of our IEEE VNC'16 poster paper [1].

mobility model is carefully simulated. Therefore, a separate vehicular traffic simulator is usually coupled with a network simulator to accurately simulate the vehicular traffic. Since most of the simulation efforts were directed to handle mobility and communication issues, security and privacy aspects were skipped in these simulators. Consequently, privacy researchers had to develop their own proposals whether in self-made or off-shelf simulators. This creates inconsistent evaluations for the proposed schemes and hardens estimating their actual performance comparatively.

However, there were two efforts that aimed to provide a generic privacy framework which are proposed in [14] and [15]. VANETsim [14] is a standalone simulator for security and privacy concepts in VANET. But it does not consider the physical characteristics of the wireless medium or the propagation of radio waves. Also, it does not support the standard VANET communication protocols which makes the obtained evaluation unrealistic when applied in the real-world environment. Eckhoff *et al.* [15] proposed a privacy assessment framework for Veins. However, they did not propose a flexible design to implement different privacy approaches nor implement popular privacy schemes to allow easy inclusion of privacy concepts in VANET simulations.

In contrast to the aforementioned works, PREXT aims at proposing a unified and extensible framework to simulate privacy schemes in VANET. The advantages of the proposed extension include:

- A modular design of a privacy layer that facilitates implementation of new privacy schemes.
- It supports seven popular privacy schemes that are based on different approaches such as silent periods, context-based and mix-zones. These built-in schemes allow non-privacy specialists to consider privacy aspects in their simulations.
- It includes an adversary module based on the nearest-neighbor probabilistic data association (NNPDA) algorithm which is able to track vehicles effectively and efficiently [16]. The strength of the adversary is fully-controlled by determining its coverage of the road network.
- Several privacy metrics are supported such as traceability, entropy, anonymity set size and pseudonyms statistics.

III. Architecture

PREXT consists of the following three main components:

1) A privacy layer inside cars that manages pseudonyms and silence periods and also communicates with mix-zone controllers.
2) A road-side unit controlling a mix-zone by advertising its location and effective range.
3) A global adversary who installs several receivers over the road network which in turn report eavesdropped messages to a central vehicle tracker.

As illustrated in Figure 1, we created a car compound module (PrivCar) that inserts a privacy layer between the application and data link layers. A sample application (PrivateSampleApp) is also developed that broadcasts beacon messages periodically. We extended the WaveShortMessage (built in Veins) by a new message called WAVEBeacon that adds other fields such as a pseudonym, velocity and a flag telling if the message is encrypted. Both the mix-zone controller and adversary receiver are modeled as RSU modules that use MxZ and Eavesdropper classes in their application layer, respectively. A network scenario can include several mix-zones and eavesdroppers which are placed according to the specified locations in the configuration file. All eavesdroppers report received messages to a central simple module, called Vehicle Tracker, which in turn removes duplicate beacons and export them in a file. The vehicle tracker can optionally run the NNPDA algorithm [6] to link beacons of changed pseudonyms to reconstruct car traces and calculate various privacy metrics. Next, we will discuss each component in detail.

A. Privacy Layer

The privacy layer is mainly formed by the BasePrivLayer class and its subclasses that handle privacy schemes. The functionalities of the privacy layer are as follows:

1) Assign the current pseudonym to messages that arrive from the application layer
2) Coordinate with mix-zone controllers and encrypt messages while the vehicle drives within the mix-zone range
3) Change the pseudonym according to the implemented privacy scheme
4) Cease sending messages down to the data link layer during silence periods

Basically, the BasePrivLayer class performs the first two functionalities while the other two should be performed by a subclass that implements a particular privacy scheme. Currently, PREXT does not include a pseudonym acquisition policy but formulates a pseudonym by concatenating the car Id (4 bytes) and a local counter (4 bytes). When a pseudonym should be changed, the local counter is incremented by one. Thus, when an application sends a message down, the BasePrivLayer class attaches the current pseudonym to it and sends it down to the data link layer. Note that messages are not actually signed or verified by other vehicles, however it might be an interesting improvement to implement a complete security architecture such as [2] to simulate the whole life cycle of pseudonyms. The BasePrivLayer class does not implement any privacy scheme and never changes the pseudonym. To do so, a new class should be created that inherits from the BasePrivLayer class as discussed in the next section.

B. Privacy Schemes

Currently, the PREXT includes the implementation of several privacy schemes such as periodical pseudonym change (PeriodicalPC) [17], random silent period (RSP) [18], coordinated silent period (CSP) [19], SLOW [20], cooperative pseudonym change scheme based on the number of neighbors (CPN) [21] and context-aware privacy scheme (CAPS) [22]. These schemes decide locally when to change a pseudonym

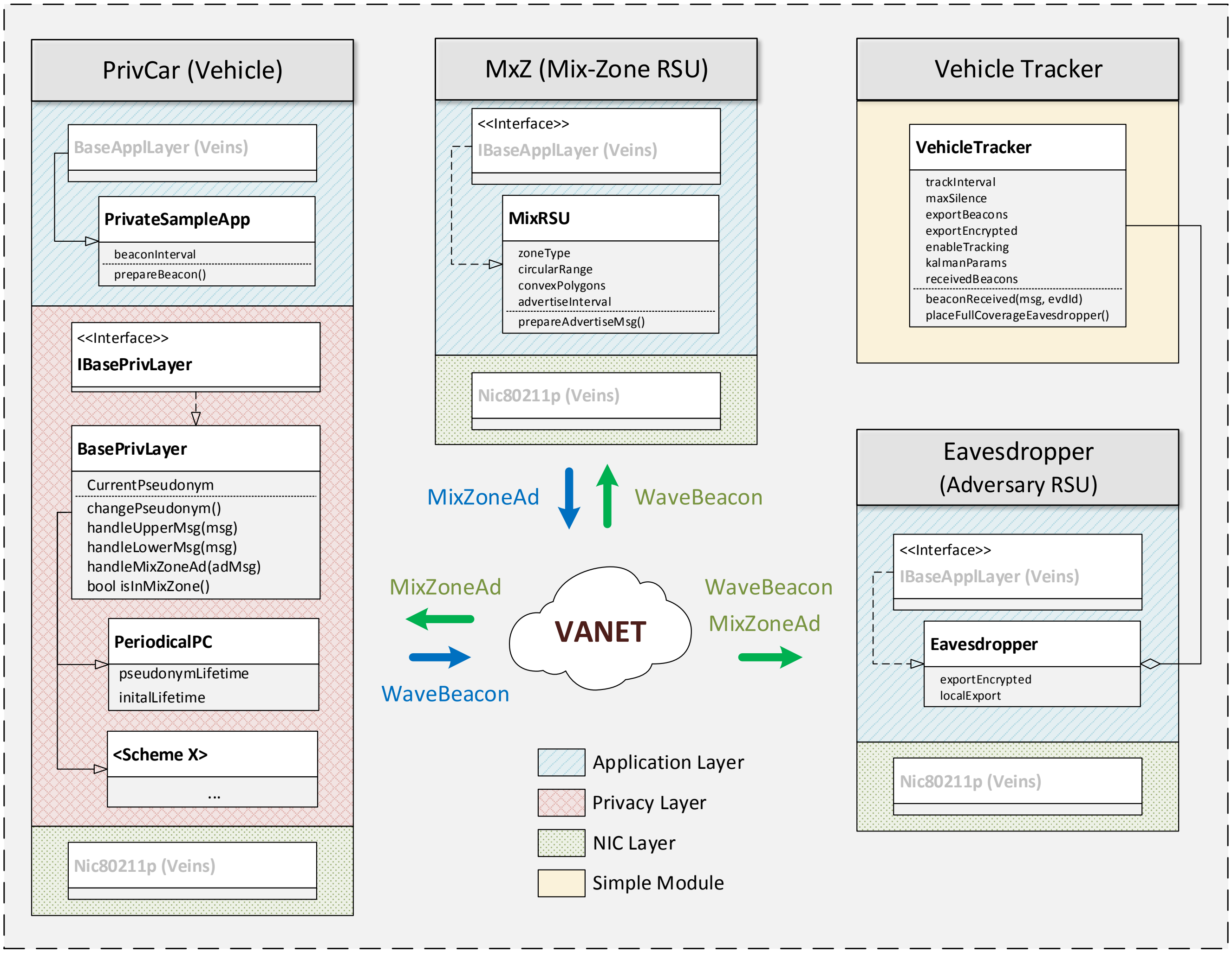


Fig. 1. Architecture of the proposed privacy extension

and how long a vehicle should be silent (if any) based on the configured parameters. In addition, the mix-zone concept [23], [24] is also implemented where vehicles are coordinated by RSUs to change pseudonyms and encrypt their messages within their effective range. Next, we will explain briefly the details of each scheme showing its parameters.

1) Periodical Pseudonym Change: Periodical scheme (PeriodicalPC) changes pseudonyms at fixed or random times. A fixed period [25] may increase simultaneous pseudonym changes among nearby vehicles although an adversary would be able to predict when pseudonyms would be changed. A random change period [17] overcomes this prediction issue but may reduce the number of simultaneous pseudonym changes.

The PeriodicalPC class can simulate both fixed and random periods. It takes as parameters the minimum and maximum pseudonym lifetimes. Internally, the PeriodicalPC class chooses a uniformly random time between both lifetimes and changes the pseudonym after that time. It chooses a new random period for every pseudonym change. When the min and max lifetimes are the same, the PeriodicalPC class simulates the fixed period case.

2) RSP: The random silent period (RSP) scheme [26] allows a vehicle to change its pseudonym after a fixed pseudonym time and keep silent for a uniformly random period within a preset range (e.g., from 3 to 13 s). It can be considered as a special type of mix zones where it is not necessary to place the zone in fixed locations.

This module takes the min and max silent time range and internally the RSP class selects a random silent period before every pseudonym change. Basically, RSP has two internal events of 1) changing pseudonym after the preset pseudonym lifetime and remaining silence and 2) exiting silence period after the randomly selected time. Each event is scheduled upon the occurrence of the other event. During silence, RSP class set the IsSilent flag and ceases any message comes from the application layer.

3) CSP: Coordinated Silent Period (CSP) is introduced by Tomandl *et al.* [19] in their comparison of silent period and mix zone schemes. CSP coordinates all vehicles in the network to remain silent and change pseudonyms synchronously. CSP seems to be theoretical since the global silence coordination among vehicles is challenging and needs further investigation to study possible implications or attacks. The delivery of packets and handling safety-critical situations during the scheduled silence are just examples that make implementing CSP in real-world scenarios challenging. However, CSP increases the privacy significantly because it maximizes the size of the anonymity set at every pseudonym change.

CSP takes two parameters which are the pseudonym life time and the silent period. In the initialization phase, CSP decides if the vehicle should be silent based on the current time and configured parameters of the pseudonym lifetime and silent time. Then, it schedules the next event whether changing the pseudonym or exiting the silence accordingly. Later on, both events are scheduled after constant intervals defined by the configured parameters.

4) SLOW: In SLOW [20], a vehicle continuously checks its current speed and broadcasts beacons only when its speed is higher than a preset threshold SP. If a vehicle does not send beacons for ST seconds, it changes its pseudonym.

5) CPN: The Cooperative Pseudonym change scheme based on the number of Neighbors (CPN) is proposed in [21]. In CPN, vehicles monitor their neighbors within radius R and wait until they reach a threshold K. When this trigger occurs, the vehicle sets an internal flag $readyFlag$, broadcasts this flag within the beacon and changes the pseudonym with the next beacon. When a vehicle receives a beacon with a set $readyFlag$ or its internal flag is set already, it changes pseudonym immediately.

The CPN class counts neighbors, through received beacons, and checks if the positions are within the configured radius. It also records if any beacon received whose $readyFlag$ is set. When a beacon is received from the application layer, CPN changes the pseudonym if the internal $readyFlag$ is set or a beacon is received whose $readyFlag$ is set since the last sent beacon. It also set the internal $readyFlag$ if the number of counted neighbors exceeds the configured threshold K.

6) CAPS: The basic concept of Context-aware Privacy Scheme (CAPS) [22] is to determine the appropriate context in which a vehicle should change its pseudonym. This approach aims at increasing the effectiveness of such changes against tracking and avoid wasting pseudonyms in easily traceable situations. Also, it determines the sufficient silence period that leads to a probable tracker confusion. It employs an internal local vehicle tracker using beacons received by its on-board communication unit.

7) Mix-zone: A mix-zone is an unobserved area where an adversary cannot observe messages broadcast by vehicles. It is typically placed at road intersections to make it difficult to predict the vehicle movements. If vehicles would change their pseudonyms within a mix zone, the adversary cannot correlate leaving vehicles with those entering the zone earlier since their messages are hidden and vehicle movements are unpredictable. Hiding messages in a mix zone is realized by keeping silence [23] or by encrypting messages using a shared key obtained from an RSU [24].

In PREXT, the mix-zone concept is implemented through encrypting beacons while vehicles are driving in the effective range of a mix-zone. Currently, there is no particular mix-zone scheme implemented but it is handled through the BasePrivLayer class in the vehicle and the MixRSU class in the RSU. This design allows evaluating double privacy approaches (i.e., silence based and mix zone based) in a single scenario by using a derived class from the BasePrivLayer class inside vehicles and placing mix-zone RSUs in the road network. The resulting heterogeneous privacy scheme will utilize the existence of mix-zones wherever deployed and still preserve privacy in the infrastructural-less regions.

The implementation of the mix-zone concept is as follows. Each mix-zone is controlled by an RSU whose a MixRSU class in the application layer. Every advertiseInterval seconds, the MixRSU class advertises the existence of the mix-zone and its effective range and shape. When a vehicle receives the advertisement message (MixZoneAd), it stores in an internal list the effective zone whether circular [24] or of particular convex polygons of non-uniform shapes [27]. When a vehicle drives within a mix-zone, the BasePrivLayer class encrypts all messages come from the application before they are forwarded to the data link layer. In fact, messages are not actually encrypted but the IsEncrypted field is only set. Messages whose IsEncrypted field is set can be exported by the eavesdropper/tracker but they are always excluded from vehicle tracking process.

IV. Adversary

The PREXT supports simulating a (global) adversary who aims at tracking vehicles by eavesdropping beacon messages. This adversary is realized by deploying receivers over the road network which report messages to a central entity for further processing. If the receivers are covering the whole road network, the adversary is considered global. Otherwise, it is called local. Both modes can be simulated in PREXT by stating the number of receivers and their locations in the configuration file. The separation concept between receivers and the central tracker allows a realistic simulation of the adversary of variant strengths represented by its coverage area. The receiver is simulated as an RSU module whose Eavesdropper class in the application layer. The central entity is simulated as a simple module called Vehicle Tracker. Next, we will discuss both entities.

A. Eavesdropper

The eavesdropper functionality is to listen to the wireless medium and report the received beacons to the vehicle tracker. The adversary may deploy many eavesdroppers to cover the road network. Depending on the placement of these eavesdroppers, beacons of one vehicle can be received by one or more eavesdropper or not detected at all. The number and placement of the eavesdroppers determine the strength of the adversary, the more spread, the stronger. The vehicle tracker

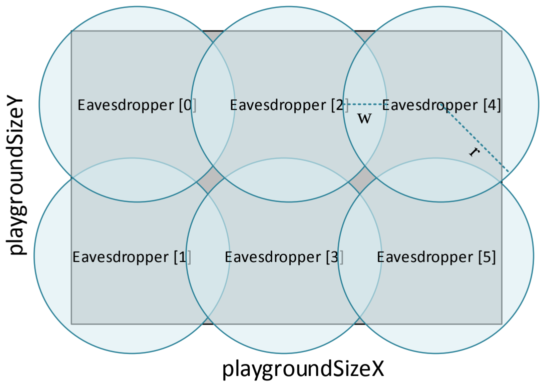


Fig. 2. (Expected) full coverage of the adversary for the road network

module can be configured to dynamically create and uniformly place eavesdroppers over the road network to achieve a likely full coverage, as illustrated in Figure 2. This feature is enabled be setting the fullCoverage parameter and controlled by two parameters. The first parameter is the expected communication range of an eavesdropper (eavesdropperRange) while the second parameter is the overlapping window between each two adjacent eavesdroppers (eavesdropperRangeOverlap). Note that a perfect coverage is not guaranteed since the configured coverage range is just an estimate from the adversary and packets can be dropped due to communication problems.

When an eavesdropper receives a beacon, it calls the beaconReceived function in the vehicle tracker module and passing the content of this beacon. We use here a direct function call for efficiency purposes, but, in reality, the eavesdropper needs a direct link to the vehicle tracker to deliver collected beacons, whether in real-time or in batches.

B. Vehicle Tracker

The vehicle tracker module is the central entity responsible for collecting beacons from different eavesdroppers and export their information after removing duplicates. It may also run the NNPDA tracking algorithm to reconstruct vehicle traces from the eavesdropped beacons and calculate various privacy metrics. This vehicle tracking feature is crucial in PREXT because it facilitates evaluating and comparing different schemes with respect to a unified (robust) adversary within vehicular environment.

When a beacon is reported by an eavesdropper, the vehicle tracker saves it in a hash table and uses the pseudonym as a key. It drops any beacon of the same pseudonym and time stamp that may be reported by another eavesdropper. Later, the tracker exports collected beacons every a preset interval (trackInterval) and calls the tracking algorithm. The hash table of beacons is then cleared to collect new beacons for the next collection step. The trackInterval parameter value should be assigned by the (maximum) beaconInterval of the vehicles. The exporting and tracking functions are enabled by setting the exportBeacons and enableTracking parameters, respectively. The vehicle tracker takes other parameters related to the tracking algorithm and Kalman filter which should not be usually changed from the default values. If the exportEncrypted parameter is set, encrypted beacons will be exported but not passed to the tracking algorithm.

The employed tracking algorithm is originally proposed in [6], [16]. It shows promising effectiveness in tracking anonymous beacons with various vehicle densities, transmit rates and position noises. Basically, the tracking algorithm consists of four iterative phases as follows:

- *State estimation* using Kalman filter which is used to obtain an accurate state for vehicles using both inaccurate measurements gained from beacons and the estimated states obtained from a predefined kinematic model.
- *Data association* using nearest neighbor probabilistic data association (NNPDA) algorithm which tries to associate each beacon to its originating vehicle by calculating an assignment probability matrix. This phase is only applied when there is one or more beacon of new pseudonyms and one or more track not assigned to a beacon using pseudonym matching. Otherwise, consecutive beacons are linked by matching similar pseudonyms.
- *Gating* phase is performed prior to the data association phase to prevent unnecessary computations for unlikely associations.
- *Track maintenance* phase is needed to handle track initiation, confirmation and deletion since number of vehicles are dynamic. This phase is further tuned than that proposed in [16] to cope with silent periods usually performed by privacy schemes. Originally, the tracker holds a vehicle track without update till *waitBfrDelete* seconds and deletes it afterwards. We added an extra parameter of the maximum silence period (*maxSilence*) that can be used by a privacy scheme. The tuned tracker only marks a vehicle track as inactive after *waitBfrDelete* time steps and holds it for additional *maxSilence*. When the tracker assigns beacons of unmatched (new) pseudonyms to the current tracks list, it only considers inactive tracks. This tweak increases the linkability of beacons since it eliminates matching beacons of new pseudonyms with unrelated tracks. If the privacy scheme does not require silence, *maxSilence* should be set to zero.

V. Scenario statistics

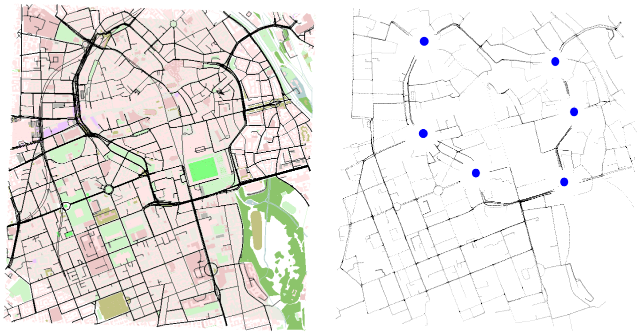
The PREXT provides many statistics that allow evaluating the simulated scenario. We employed OMNeT++ signals to expose statistics from different modules which provide flexibility in how data is finally recorded. In addition, the vehicle tracker module produces scalar and vector statistics for privacy evaluation. Table I provides definitions for important statistics of each module.

VI. Evaluation

In this section, we evaluate the PREXT showing its efficiency and the performance of the implemented schemes in

TABLE I
Selected statistics provided by PREXTmodules

Module	Statistic	Definition
BasePrivLayer	vehicleLifeTime	Total time the vehicle appears in the simulation
	psynmTimes	An array of the pseudonym lifetimes
	mixZoneTimes	An array of time periods in which a vehicle is engaged with mix-zones and its beacons are encrypted
Eavesdropper	nBeacons	Total number of beacons received by this eavesdropper
	nPseudonyms	Total number of distinct pseudonyms encountered by this eavesdropper
VehicleTracker	MonitorTime	An array of the time differences between the first and last beacon of each vehicle monitored by the tracker.
(Signals)	maxEntropy	An array of the max entropy encountered by each vehicle during the whole simulation
	maxAnonymitySetSize	An array of the max anonymity set size encountered by each vehicle during the whole simulation
	nTrackerConfusion	A histogram of the number of tracker confusions per vehicle
	ContTrackingTimePer	A histogram of the percentage of the continuously tracked to the total number of beacons of each vehicle
(Scalars)	nTraces	Total number of vehicles encountered by the tracker
	nTracesChngPsynms	Total number of vehicles encountered by the tracker and changed their pseudonyms at least once
	Traceability90	Traceability metric defined in [28]
	N_Traceability90	Normalized traceability metric defined in [28]


(a)

(b)

Fig. 3. (a) Munich city center map. (b) Accumulative vehicle positions extracted from their *unencrypted* beacons with the existence of 6 circular mix-zones (blue circles). Cuts in the traces can be noticed around the effective range of mix-zones (150 m).

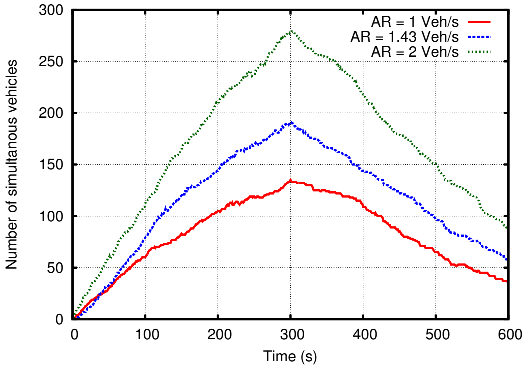


Fig. 4. Vehicle density over simulation time of 10 min in various arrival rates (AR).

reducing traceability. Hereafter, we assume each vehicle has only one trace in the traces dataset and we use vehicle and trace terms interchangeably.

A. Simulation Setup

We employed a road map of Munich city center whose size of 2.67 km x 2.8 km, as shown in Figure 3(a). This map is obtained from OpenStreetMap and converted into a SUMO network using netconvert and polyconvert tools included in the SUMO 0.25.0. We adopted the recommended options specified in the SUMO Wikipages [29]. Then, we used the randomTrips script to generate random vehicle trips and traces with variant arrival rates of 1, 1.43 and 2 vehicles per second. These arrival rates generate a total number of traces of 169, 234 and 327, respectively. Vehicles are successively arriving for 5 min then another 5 min are left to let vehicles exit the simulation, as shown in Figure 4. The max speed is 50 km/h with an acceleration range from -4.5 m/s^2 to 2.6 m/s^2. The median trace lifetime is 290 s, while the median trace distance is about 2 km. Each experiment is repeated 5 times with a different random seed. The PrivSampleApp is used in vehicles in all experiments to let vehicles broadcast beacons every 1 s. To let beacons reach eavesdroppers without communication problems, we reduced the obstacle shadowing to 0.1 dB per cut and 0.0001 dB per meter. These shadowing values are not realistic and should be reconfigured when simulating real-world scenarios. In this case, the full coverage mode of the adversary should be avoid as well, because it does not consider the location of the eavesdropper nodes if they are inside buildings or in a free-space beside the road. This factor will significantly affect the eavesdropping capability of the adversary. Table II shows simulation parameters used in the experiments.

B. Performance Evaluation

The first experiment evaluates how efficient the PREXT compared with a pure Veins simulation. We run multiple simulations, one for each privacy scheme, with a full-coverage adversary and another simulation that uses Veins basic modules. However, in this Veins simulation, vehicles use the PrivSampleApp class in their application layer to broadcast beacons every second. We run our experiments on an Intel QuadCore i7-4800MQ @ 2.70GHz CPU. In fact, we run the experiment sequentially on one core to avoid any synchronization overheard.

TABLE II
SIMULATION PARAMETERS

Module	Parameter	Default Value
Veins	Transmission power	20mW
	Bit rate	18 Mbps
	Thermal noise	-110 dBm
	Packet header length	256 bit
	Beacon payload length	100 byte
	Beacon rate	1 Hz
Tracker	Eavesdropper range	300 m
	Eavesdropper overlap	30 m
	Track interval	1 s
Periodical	Pseudonym lifetime	60 s
RSP	Pseudonym lifetime	60 s
	Silent period	(3, 9) s
SLOW	Speed threshold	8 m/s
	Silent threshold	5 s
CPN	Radius	100 m
	Neighbors threshold	2
CAPS	Pseudonym Range	(60, 180) s
	Silence Range	(3, 13) s
	Missed beacons silence threshold	2 beacons
	Neighborhood radius	50 m
Mix-zone	Advertisement Interval	3 s
	Zone shape	Circular
	Zone range (radius)	150 m
	Number of zones	6
	Locations	see Figure 3(b)

Figure 5 shows the running time of these simulations with different arrival rates. It is noticed that the Periodical and CPN schemes run slower than the case of using no privacy modules "No Scheme" (12% and 15% slower, respectively on average). This delay comes from the overhead of the privacy layer and adversary modules. The RSP scheme runs almost as efficiently as "No Scheme" case because silence periods reduce the amount of packets that should be processed which compensates the scheme and tracker overhead. This behavior is maximized in SLOW scheme (30% faster) because there is a huge number of beacons that are eliminated which reduces the simulation overhead significantly. In CAPS, the overhead of the in-side trackers slightly increased the running time so that it becomes as efficient as CPN. The mix-zone scheme has the highest overhead (30% slower) because of the additional advertisement messages sent from RSUs and the computational overhead made by vehicles to check their existence within the mix-zone range. Although of this overhead, the simulation can still run in real-time for intermediate vehicle densities.

C. Schemes Comparison

In this section, different privacy schemes are evaluated against each other in terms of the (normalized) traceability. As defined in [28], traceability measures how effective an adversary can track a vehicle continuously for more than 90% of its trace. This continuous tracking is necessary to practically breach the driver privacy because traces de-anonymization needs complete trajectories with allowable errors around endpoints. Normalized traceability is calculated similarly but with neglecting traces that never changed their pseudonyms. Traceability and normalized traceability of privacy schemes are shown in Figures 6(a) and 6(b), respectively. Schemes parameters are specified in Table II.

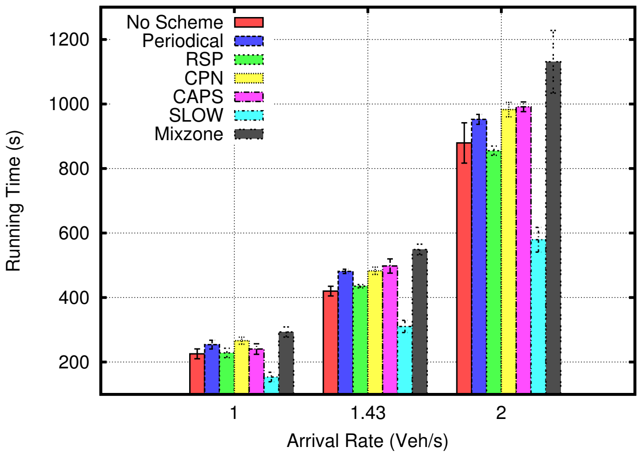
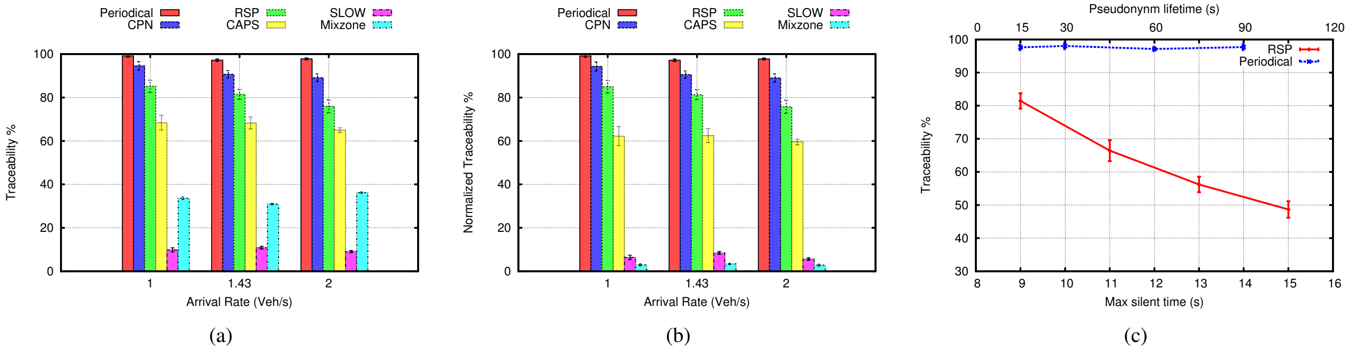


Fig. 5. Running time of simulations of different schemes in three different arrival rates.

Periodical and CPN schemes cannot reduce traceability (up to 90% regardless the arrival rate) because they don't employ any discontinuity in the spatiotemporal information broadcast in beacons. Also, CPN scheme consumed a large number of pseudonyms during simulation (i.e., 10 to 16 pseudonym per minute in the lowest and highest arrival rates, respectively). RSP scheme reduces traceability a little bit due to the silent periods used before a pseudonym change. The reduction in traceability is closely related to the length of the silence period as shown in Figure 6(c). This figure shows the traceability of RSP with various silent times. It is noticed that the traceability is significantly reduced with the increase of the length of silence period. It is also worth to mention that restricting parameters do not always result in reduced traceability. For example, we add an evaluation for the Periodical scheme with shorter pseudonym times down to 15 s. It is noticed that traceability is still high regardless the pseudonym lifetime. CAPS reasonably reduces the traceability since it selects the effective contexts for pseudonym change that cause tracker confusions.

SLOW scheme reduces traceability significantly up to 10%. However, SLOW makes vehicles silent for almost 45% of their lifetime on average. This silence reduces the targeted traffic awareness and may negatively impact the functionality of safety applications as shown in [30]. Mix-zone scheme reduces traceability given that a vehicle pass by it. We notice about 30% of vehicles do not pass by any mix-zone, although they are placed in central intersections on the map. Also, it is worthy to note that this traceability can be much enhanced by timing and transition attacks that are not yet implemented in PREXT. Related studies, such as [23], show that these attacks can achieve a tracking success probability of 60% on average.



(a) (b) (c)

Fig. 6. (a) Traceability (b) Normalized Traceability of the privacy schemes in various arrival rates. (c) Traceability of Periodical and RSP schemes in the intermediate arrival rate (1.43 Veh/s)

VII. Conclusion

A privacy extension for Veins framework is proposed and evaluated in this paper. Its flexible design supports implementing several privacy schemes of different approaches such as silent period (RSP and CSP), context-based (CPN, CAPS and SLOW) and mix-zones. It includes an adversary which can collect and track beacon messages and reconstruct vehicle traces. It also evaluates the preserved privacy in terms of several popular metrics such anonymity set size, entropy and traceability. According to the aforementioned experiments, PREXT does add a significant delay to the simulation time except mix zone based schemes. However, the simulation can still run in real time in low and intermediate vehicle densities. In future work, we will use the proposed extension to develop a hybrid privacy protocol that uses the appropriate privacy scheme according to the vehicle context.

References

[1] K. Emara, "Poster: PREXT: Privacy Extension for Veins VANET Simulator," in *Vehicular Networking Conference (VNC), 2016 IEEE*, ser. VNC'16. IEEE, 2016.

[2] M. Khodaei and P. Papadimitratos, "Evaluating on-demand pseudonym acquisition policies in vehicular communication systems," in *Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet*, ser. IoV-VoI '16. New York, NY, USA: ACM, 2016, pp. 7–12. [Online]. Available: http://doi.acm.org/10.1145/2938681.2938684

[3] "ETSI TS 102 941 V1.1.1," *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*, Jun 2012.

[4] "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.

[5] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on*, Feb. 2010, pp. 176 –183.

[6] K. Emara, W. Woerndl, and J. Schlichter, "Vehicle tracking using vehicular network beacons," in *Fourth International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN)*, Madrid, Spain, Jun. 2013.

[7] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proceedings of the 7th International Conference on Pervasive Computing*, ser. Pervasive '09. Berlin, Heidelberg: Springer-Verlag, May 2009, pp. 390–397.

[8] H. Zang and J. Bolot, "Anonymization of location data does not work: A large-scale measurement study," in *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '11. New York, NY, USA: ACM, 2011, pp. 145–156.

[9] 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, January 2011.

[10] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of sumo–simulation of urban mobility," *International Journal On Advances in Systems and Measurements*, vol. 5, no. 3&4, 2012.

[11] M. Piórkowski, M. Raya, A. L. Lugo, P. Papadimitratos, M. Grossglauser, and J.-P. Hubaux, "Trans: Realistic joint traffic and network simulator for vanets," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 12, no. 1, pp. 31–33, Jan. 2008. [Online]. Available: http://doi.acm.org/10.1145/1374512.1374522

[12] J. Härri, M. Fiore, F. Filali, and C. Bonnet, "Vehicular mobility simulation with vanetmobisim," *Simulation*, vol. 87, no. 4, pp. 275–300, Apr. 2011. [Online]. Available: http://dx.doi.org/10.1177/0037549709345997

[13] M. Rondinone, J. Maneros, D. Krajzewicz, R. Bauza, P. Cataldi, F. Hrizi, J. Gozalvez, V. Kumar, M. Rckl, L. Lin, O. Lazaro, J. Leguay, J. Hrri, S. Vaz, Y. Lopez, M. Sepulcre, M. Wetterwald, R. Blokpoel, and F. Cartolano, "itetris: A modular simulation platform for the large scale evaluation of cooperative {ITS} applications," *Simulation Modelling Practice and Theory*, vol. 34, pp. 99 – 125, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1569190X1300018X

[14] A. Tomandl, D. Herrmann, K. P. Fuchs, H. Federrath, and F. Scheuer, "Vanetsim: An open source simulator for security and privacy concepts in vanets," in *High Performance Computing Simulation (HPCS), 2014 International Conference on*, July 2014, pp. 543–550.

[15] D. Eckhoff, M. Protsenko, and R. German, "Toward an open source location privacy evaluation framework for vehicular networks," in *2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*, Sept 2014, pp. 1–2.

[16] K. Emara, W. Woerndl, and J. Schlichter, "Beacon-based Vehicle Tracking in Vehicular Ad-hoc Networks," TECHNISCHE UNIVERSITÄT MÜNCHEN, Tech. Rep., Apr. 2013. [Online]. Available: http://mediatum.ub.tum.de/attfile/1144541/hd2/incoming/2013-Apr/691293.pdf

[17] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random pseudonym change scheme in vanets," *Cluster Computing*, vol. 17, no. 2, pp. 413–421, 2014. [Online]. Available: http://dx.doi.org/10.1007/s10586-012-0242-7

[18] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 2, March 2005, pp. 1187–1192 Vol. 2.

[19] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation-based evaluation of techniques for privacy protection in vanets," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on*. IEEE, 2012, pp. 165–172.

[20] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A Practical pseudonym changing scheme for location privacy in VANETs," in *2009 IEEE Vehicular Networking Conference (VNC)*. IEEE, Oct. 2009, pp. 1–8.

[21] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the

number of neighbors in {VANETs}," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599 – 1609, 2013.

[22] K. Emara, W. Woerndl, and J. Schlichter, "CAPS: Context-Aware Privacy Scheme for VANET Safety Applications," in *Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '15. New York, NY, USA: ACM, 2015.

[23] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *Proceedings of the 4th European Conference on Security and Privacy in Ad-hoc and Sensor Networks*, ser. ESAS'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 129–141. [Online]. Available: http://dl.acm.org/citation.cfm?id=1784404.1784417

[24] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks," in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, Vancouver, Aug. 2007.

[25] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "Slotswap: strong and affordable location privacy in intelligent transportation systems," *Communications Magazine, IEEE*, vol. 49, no. 11, pp. 126 –133, Nov. 2011.

[26] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "Caravan: Providing location privacy for vanet," in *in Embedded Security in Cars (ESCAR*, 2005.

[27] B. Palanisamy and L. Liu, "Attack-resilient Mix-zones over Road Networks: Architecture and Algorithms," *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 495–508, 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6815691

[28] K. Emara, W. Woerndl, and J. Schlichter, "Context-based Pseudonym Changing Scheme for Vehicular Adhoc Networks," *ArXiv e-prints. 1607.07656*, Jul. 2016.

[29] "SUMO Wiki Page," http://sumo.dlr.de/wiki/Networks/Import/OpenStreetMap, [Online; accessed Aug-2016].

[30] K. Emara, "Safety-aware location privacy in vehicular ad-hoc networks," Ph.D. dissertation, München, Technische Universität München, 2016.