SlotSwap: Strong and Affordable Location Privacy in Intelligent Transportation Systems

David Eckhoff and Reinhard German, University of Erlangen
Christoph Sommer and Falko Dressler, University of Innsbruck
Tobias Gansen, Audi Electronics Venture GmbH

ABSTRACT

Public acceptance, and thus the economic success, of an ITS is highly dependent on the quality of deployed privacy mechanisms. In general, neither users nor operators should be able to track a given individual. One approach to facilitate this is the usage of pseudonym pools, which allow vehicles to autonomously switch between different identities. We extend this scheme with that of a time-slotted pseudonym pool of static size, reducing the storage and computation needs of the envisioned ITS while further improving users' privacy. In addition, we allow the exchange of pseudonyms between vehicles, eliminating the mapping between vehicles and pseudonyms even for the ITS operator. We support the exchange of both current and future pseudonyms, further enhancing users' privacy. We evaluate the feasibility of our approach and back up privacy claims by performing a simulative study of the system using the entropy of nodes' anonymity sets as the primary metric.

INTRODUCTION

Equipping vehicles with wireless devices to create an intelligent transportation system (ITS) offers a wide range of possible applications — efficiency applications like traffic information systems (TISs) or safety-relevant systems such as driving assistance or intersection management are just two of many envisioned in the near future. Many of these applications require vehicles to periodically broadcast their whereabouts along with speed and other information to function properly [1]. These beacon messages are usually referred to as cooperative awareness messages (CAMs), as they enable other vehicles to be aware of their surroundings and, for example, allow safety applications to provide drivers with valuable information. Periodically sending beacon messages, however, raises some privacy concerns.

If an adversary is able to overhear vehicles' beacon messages at multiple locations (e.g., by deploying several wireless access points), it could be able to collect or aggregate this data and thus track all vehicles in these regions. This can severely compromise the privacy of users, because vehicles are usually only driven by very few different drivers [2]. By further correlating origin, destination, and time of the recorded tracks, it might even be possible to link a track to a specific individual.

This is further compounded by the fact that wide-area deployment of roadside units (RSUs) is a prerequisite for successful operation of TIS services at low penetration rates, especially in the rollout phase, where only a few vehicles are equipped with wireless devices. Such RSUs will be operated by a very limited number of system providers. In a worst case scenario, it is exactly these RSUs that could be exploited to track entities throughout the network, therefore posing a serious threat to the location privacy of participating drivers. This allows an operator or any other user to create accurate traces of all participants if the number of observations is high enough [3].

The ITS community is well aware of the privacy challenges that accompany Car-to-X technology, and a wide range of approaches to overcome these issues have been proposed. What most of them have in common is that vehicles first have to get rid of a static identifier to be used in broadcast messages. Naturally, reusing the same identifier over a longer period of time makes tracking easier, as two observations, regardless of their temporal or local correlation, can be mapped to one and the same vehicle.

The state of the art, and also what is being done in current field operational tests, is the use of multiple pseudonyms instead of static identifiers [4]. This is commonly realized by means of a public key infrastructure (PKI). Vehicles are usually equipped with a base identity, which

0163-6804/11/$25.00 © 2011 IEEE

allows for requesting pseudonyms from a central certificate authority, usually operated by the system provider. At the same time, this base identity allows for the participation of a vehicle in the network. Pseudonyms are certificates that are only valid if they are signed by a root certificate authority (CA) and only for a limited time. Without a mechanism like this, it is difficult to prevent freeloaders or known adversaries from participating in the system. After obtaining pseudonyms, vehicles (i.e., *nodes* in the wireless network) can then autonomously select a pseudonym for communication to complicate tracking of their positions.

A consequential approach would be to use a different pseudonym for every message to preserve a very high level of privacy, similar to not using source addresses at all. However, many (safety) applications have to link two or more successive beacon messages to one vehicle in order to function properly [5]. Overcoming this problem by simply changing the pseudonym every n seconds has been shown to offer only marginal protection of users' location privacy [6]. Therefore, the next logical step is to deploy a pseudonym change strategy that also accounts for the environment in which a vehicle is. When position, speed, heading, and the number of cars in transmission range are accounted for when changing pseudonyms, a much higher level of location privacy can be reached, as it reduces the chances for an attacker to successfully follow a pseudonym change [7].

Combining situation-aware strategies with additional silent periods is a promising approach to further protecting participating drivers: after changing a pseudonym, the vehicle will stop emitting beacon messages for a random amount of time, making it even harder for an adversary to follow such a change [8]. This is, however, a perfect example of the interference of privacy schemes with safety applications, which many believe is an inevitable trade-off. Both silent periods and pseudonym changes, when performed at high-density spots mostly found at intersections or traffic lights, can make a vehicle indistinguishable from others because even complex tracking algorithms may fail there [3]. Unfortunately, these are the very situations where safety applications are needed most in urban environments.

Another issue of these approaches is the use of a CA, which signs the pseudonym certificates and is therefore able to resolve every pseudonym to the static base identity of a vehicle and can hence track every vehicle as long as it is able to overhear beacon messages. One possible way to deal with this problem is the separation of the CA into a *privacy authority* and an *identity authority*, both sharing just parts of the identities, hence requiring their cooperation to resolve an identity [9]. This idea of *separation of concerns* is by design susceptible to abuse as it is very hard for users to check whether these policies are actually enforced.

In the context of mobile ad hoc networks (MANETs), the problem of a "Big-Brother-CA" has been dealt with by the exchange of pseudonyms [7] between mobile nodes. We adopt and extend this idea, apply it to vehicular networks, and make it part of the privacy approach we present in this article.

When designing privacy schemes for vehicular networks, important domain-specific constraints have to be kept in mind. Almost all of the discussed approaches need a large pool of pseudonyms, so that if the CA is not reachable due to lack of connectivity, or the car has not been used for a long time period, the vehicle can still send messages until the CA supplies new pseudonyms.

A larger number of pseudonyms stored on each vehicle can therefore decrease the possibility of a car not being able to transmit messages, but the required disk space, transfer volume, and management costs will also significantly increase. If the network grows, there will be a considerable computational and network overhead at the CA just to keep all nodes equipped with a sufficient number of pseudonyms.

In this article, which is an extension of our work presented in [10], we build on the described pseudonym-based solutions and introduce SlotSwap, a system that offers both low-bandwidth pseudonym management and unlinkability of pseudonyms, thus, by design, providing strong privacy for all participants in the ITS.

In order to achieve this, we employ time-slotted pseudonym pools, which substantially reduce network and computational load for the operator, and introduce static upper bounds for disk space usage and communication overhead between vehicles and CA. In addition, we combine this approach with the concept of pseudonym exchange of both the currently used pseudonym and those of future time slots to further improve the level of privacy enjoyed by drivers and to counter the ability of system providers to map pseudonyms to unique base identifiers. We present a communication protocol followed by a discussion of problems and possible attacks, and evaluate the offered privacy using nodes' entropy. As can be seen from the results, the achieved entropy is much higher than in related approaches. We show that our pseudonym exchange scheme is a feasible approach for ITS deployments.

We build on the described pseudonym-based solutions and introduce SlotSwap, a system that offers both low-bandwidth pseudonym management and unlinkability of pseudonyms, thus, by design, providing strong privacy for all participants in the ITS.

Time-Slotted Pseudonym Pools and Pseudonym Swapping

Instead of storing a very large amount of pseudonyms, every node maintains a time-slotted pseudonym pool with slot length t. For each time slot, there is exactly one assigned pseudonym. The total period length p and p/t time slots result in p/t pseudonyms per car with only one valid pseudonym for every arbitrary point in time. When a time slot has passed, each node will change its pseudonym. This can be achieved by clocks roughly synchronized with the GPS signal.

While the use of non-overlapping pseudonyms, as also proposed in [11], is very similar to time slots, nodes in our scenario will reuse pseudonyms. When the last p/t-th time slot has passed, time slot 1 will become active again, meaning that the time period will simply restart from the beginning.

It has been shown that the exchange of pseudonyms between nodes can increase privacy in mobile networks and complicate tracking for an adversary. If nodes are able to exchange their pseudonyms in secrecy by using encryption, a possible mapping at an authority will also become invalid.

A straightforward choice for those values, t = 10 min and p = 1 week, results in a pseudonym being valid for, say, Monday from 6:00 a.m. till 6:10 a.m. Note that this pseudonym is then, in fact, valid on every Monday for the said 10 min. It can be seen that the only parameter for time-slotted pools, which has a direct influence on location privacy during a trip, is the time slot length t, which determines how often a node changes its pseudonym.

It has been shown that the exchange of pseudonyms between nodes can increase privacy in mobile networks and complicate tracking for an adversary [7]. If nodes are able to exchange their pseudonyms in secrecy by using encryption, as proposed in the WAVE standard, and to keep third parties from tracking which nodes have swapped pseudonyms, a possible mapping at an authority will also become invalid. Due to the time-slotted pseudonym scheme, only pseudonyms valid for a specific time slot can be exchanged; otherwise, it cannot be guaranteed that every vehicle has exactly one pseudonym per time slot. This means that, P_n being the pseudonym valid for time slot n, two vehicles must only exchange pseudonyms P_n with P'_n.

Swapping the currently used pseudonym with another node is not trivial, as the exchange partner has to be chosen carefully so that both vehicles can benefit from an exchange in terms of location privacy. For example, two cars passing, each going in a different direction, will most likely not increase their anonymity by swapping pseudonyms because this action could easily be detected due to the unlikeliness of both cars having turned around at the same time. To effectively gain anonymity from a pseudonym exchange, nodes have to take context information into account [12]. This means that a node evaluates its environment and then decides if changing its pseudonym is profitable, so an adversary cannot simply infer the nodes' pseudonyms after the exchange by extrapolating their expected position based on their last known heading and speed [6].

In our approach, we use the speeds, headings, and positions of other vehicles to determine whether a node A will ask a node B in its vicinity to exchange the currently valid pseudonym. For the remainder of this article, we refer to all nodes meeting these requirements as *candidates*.

By carefully choosing bounds for similarity, we increase the likelihood of both exchange partners being indistinguishable in terms of position. An adversary then cannot be sure whether a pseudonym exchange has taken place or not. The efficiency of this scheme, of course, is highly dependent on the frequency and positional accuracy of the beacons each car emits. The privacy achieved by this approach could thus be amplified by using further privacy enhancing methods, such as random silent periods [8], where both cars will not send beacons for a certain amount of time after a possible exchange.

However, one problem remains: If vehicles only exchange currently valid pseudonyms (i.e., their current identifier), each vehicle will start using the same pseudonym every p/t slots, because once a new slot $n + 1$ has begun, the pseudonym last used in slot n will not be touched or exchanged again until this slot is active again. This way an attacker or a system provider is able to link two locations to one node: the present one (e.g., this Monday 6:00:00 a.m.) and the one from the last time the time slot was active (e.g., last Monday 6:09:59 a.m.). Furthermore, each time a car enters a time slot for the first time, which will happen p/t times after being equipped with the onboard unit, the operator of the CA can link the first location in these time slots to a vehicle. It has been shown that accumulated information about vehicles can be used to create traces and profiles for a user [13].

Therefore, cars have to be able to exchange these pseudonyms *before* actually using them. To achieve this, each time a time slot ends, the last used pseudonym is marked as *traceable*. Similarly, all pseudonyms that are freshly obtained from the CA are marked as traceable. When a node encounters another node, it decides to exchange either the current pseudonym (if the other node is a *candidate*) or one marked traceable, removing the flag if successful. Preferably the currently active pseudonym is exchanged, as it directly increases the level of location privacy for both users. However, for the exchange of other pseudonyms, constraints like speed or heading can be neglected, due to the fact that an attacker is not able to decrypt the transmitted data and determine for which slot pseudonyms were exchanged.

To reiterate, it has been shown that too frequent pseudonym changes can have a negative impact on safety applications and geographic routing in vehicular networks [5]. We therefore allow only one pseudonym exchange per car every 60 s. In addition, to avoid overloading the network, node A must only contact node B every 20 s.

Cooperative awareness messages as emitted by vehicles in an ITS will be broadcast unencrypted. Therefore, an overhearing adversary can conclude if node A is a candidate for node B and thus anticipate the exchange of the current pseudonym. To overcome this predictability, we introduce a 50 percent probability to decide whether a node will send a positive response. This means that if node A asks for the exchange of the currently active pseudonym, node B will accept *or* reject the request. If the request is rejected, nodes B and A will exchange another pseudonym instead so that an attacker cannot determine if the nodes have swapped their current pseudonyms simply based on message sizes.

Figure 1 depicts possible flows of the pseudonym exchange process. Vehicle A requests an exchange of the currently valid pseudonym from vehicle B, because both vehicles happen to have similar values for heading, speed, and position. In half of all cases, node B will respond with its current pseudonym, and A will finalize the exchange process by handing over its current pseudonym as well. The vehicles will then use the new pseudonyms. Alternatively, vehicle B will not exchange its current identifier, but respond with another pseudonym from its pool, preferably one marked as traceable. Vehicle A will accept this, and answer with the corresponding pseudonym from its own pool. Both vehicles will replace their old pseudonym for the given

slot with the one from the other node and continue using their current identifier.

Benefits and Limitations

An advantage of the time-slotted approach over huge pseudonym pools is its property to ensure that, ideally, a vehicle always has a pseudonym to participate in the ITS as long as it has received its p/t pseudonyms in the setup phase. Even if the CA is not reachable or the car is not used for a long time period, the vehicle will not run out of pseudonyms because it can reuse the old ones.

In addition, our scheme introduces upper limits for disk space and, more important, traffic volume. This simplifies the design of onboard units and also reduces the communication costs, making the deployment of an ITS more affordable. The pseudonym pool size is reduced to a constant value of p/t times the size of a pseudonym; more important, the workload at the CA is no longer dependent on the number of nodes actually participating in the network, but rather on the ones joining it.

Using time slots and GPS-synchronized clocks, every node will change its pseudonym at the same time. Depending on penetration rate and traffic density, this can increase drivers' privacy, as we show in our evaluation. By further applying a pseudonym exchange scheme, the privacy of users can be substantially increased. Allowing the exchange of current and future pseudonyms eliminates the mapping at an authority and allows nodes to start new time slots already anonymously.

Accountability in pseudonym exchange environments remains an open problem. Therefore, the use of our scheme should be limited to non-safety-critical messages to avoid misuse. The class of "critical safety messages" includes messages such as accident and emergency break messages. We argue that for non-critical service messages, but also for periodic beaconing, preservation of unlinkability and privacy is more important than accountability.

While, by design, in our scheme every node has only one valid pseudonym for any point in time, the use of tamper-proof devices is crucial. Tampered onboard units could be configured not to delete old pseudonyms after exchanging them with another node, allowing an adversary to build up a pool of many pseudonyms, all valid for the same time slot.

Evaluation

There are different metrics to measure the level of location privacy enjoyed by an individual in a network. Anonymity, in our case the precondition for location privacy, is interpreted by Pfitzmann and Hansen as the "state of being not identifiable within a set of subjects, the anonymity set" [14]. The anonymity set hence contains all nodes in the network that could possibly be a targeted individual. However, in our network, not all of these nodes are equally likely to be this individual, meaning the size of the anonymity set alone is not a sufficient metric to measure the location privacy. Instead, we use the entropy, as

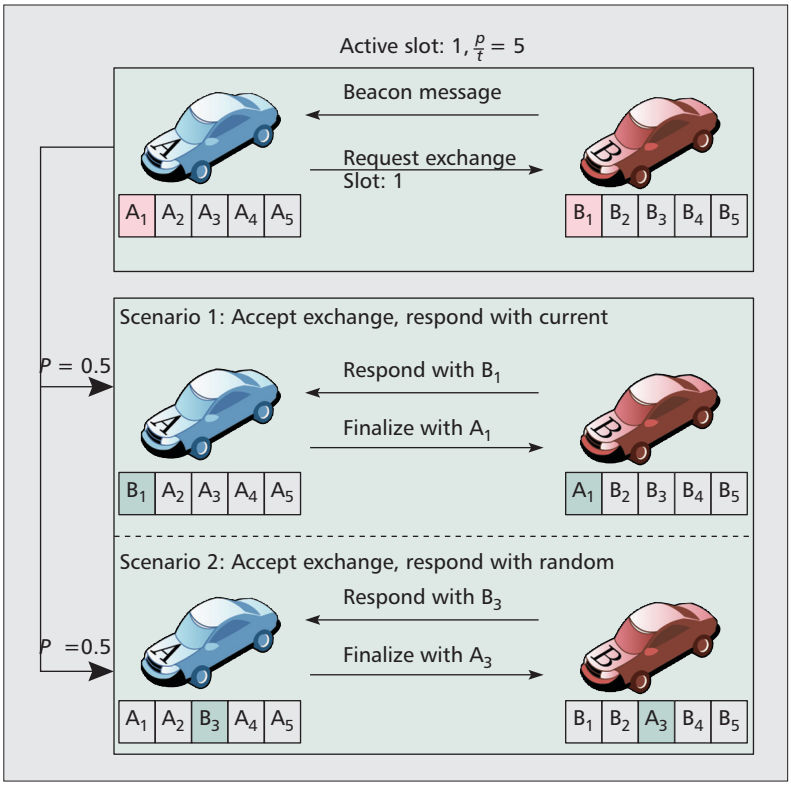

Figure 1. *Pseudonym exchange between two cars: The currently valid pseudonym is requested and confirmed in scenario 1 (resulting in the change of the current pseudonym), but rejected and answered with a random pseudonym from the pool in scenario 2.*

used in information theory, of the anonymity set, which can be seen as the uncertainty in determining the current identifier of an individual [15].

In order to calculate the entropy, let p_i be the probability of node i to be target I, the sum of all probabilities p_i being 1. The entropy H of identifying an individual driver in the anonymity set S is then defined to be

$$H = -\sum_{i=1}^{|S|} p_i \times \log_2 p_i .$$

The upper limit of H (i.e., the maximum value of entropy for a given individual) is attained for all entities in S equally likely to be the targeted driver, and can be calculated to be $\log_2 |S|$. However, this is almost impossible to achieve in an ITS, because nodes may contact a large number of other nodes, and the relation *A has met B* is rarely transitive.

A simple example serves to illustrate how to interpret entropy values for a given individual. Assuming an attacker is not sure whether the individual uses identifier A or B, and both nodes are equally likely to be the target, the anonymity set for the individual is $S = \{0.5, 0.5\}$. The entropy H is thus 1. On the other hand, if individual I is with a certainty of 80 percent the driver of A and with 20 percent the driver of B, the anonymity set would be $S = \{0.8, 0.2\}$ and the resulting entropy $H \approx 0.72$. If we were to consider three nodes, each equally likely to be the target, the anonymity set is $S = \{0.33, 0.33, 0.33\}$ and the entropy $H \approx 1.5$.

The evaluated level of location privacy enjoyed by an individual is always relative to the power of an attacker trying to track a specific person in the network. In our simulations, we assume a global passive attacker, that is, an attacker that is able to overhear every message sent in the network.

Attacker Model

The evaluated level of location privacy enjoyed by an individual is always relative to the power of an attacker trying to track a specific person in the network. In our simulations, we assume a global passive attacker, that is, an attacker that is able to overhear *every* message sent in the network. The attacker is further able to evaluate the content of all broadcast beacon messages (which we assume to include the speed, position, and heading of a node). As the attacker is, of course, well aware of the protocol, it is able to conclude which nodes might exchange their current pseudonyms. The attacker is, however, not able to actually follow the pseudonym exchange, as all of these messages are encrypted using public key cryptography. What the attacker can gather from observing transmissions in the network is the fact that pseudonym requests and replies have been exchanged.

Our attacker model is based on the strong assumption that at the beginning of the lifetime of a node, the attacker can link an individual to the vehicle. If this was not the case, the individual would already be anonymous from the start and could only be exposed through origin/destination pairs if tracking throughout the network was successful.

When modeling an attacker using tracking algorithms, the apparent strength of the attacker is heavily dependent on the used mobility and driver model. If, for example, nodes do not change lanes or drive in a very predictable manner, tracking algorithms will perform significantly better. Therefore, we choose to use a probabilistic attacker model.

As we have shown, the entropy is based on values of p_i. However, the distribution of p_i is directly dependent on the strength of an attacker. The attacker strength is defined as the probability with which an attacker is able to follow a pseudonym exchange between two nodes. The weakest possible attacker in our scenario would thus be an attacker that is not able to track a pseudonym exchange. This means that from the adversary's perspective, an individual I, previously known to be the driver of A, is equally likely to be the driver of A or B after these vehicles have exchanged their current identifier.

The strongest possible attacker cannot be confused by pseudonym exchanges and is therefore able to track every entity throughout the network. Obviously, the entropy H for each individual in the network would then be zero. The attacker strength also affects by how much the level of privacy is increased when a new slot in the slotted pseudonym pool becomes active (i.e., when all nodes will start using new pseudonyms). If we assume that two nodes very close to each other could confuse an attacker by exchanging their pseudonyms (the extent being dependent on its strength), this attacker will also be confused when these two nodes both switch to a new pseudonym simultaneously. From this we follow that the level of confusion is based on the amount of candidates directly neighboring a node. NB: Not all cars within transmission range are considered *candidates*, only those with similar speed, heading and position. For a more detailed description of the used attacker model please refer to [10].

Simulation Setup

We investigated our scheme with the help of our *Veins*[1] simulation environment [16], which is based on two simulation toolkits, both well established in their respective domain. Highly detailed vehicular mobility models, in particular with regard to intersection management, were provided by SUMO, a dedicated traffic microsimulation toolkit from the domain of traffic engineering. We further implemented the presented protocol for pseudonym exchange in the network simulator OMNeT++ using its INET Framework extension to simulate wireless transmissions.

For the evaluation, we chose the following protocol parameters: A node may not change its current pseudonym more often than once every 60 s. Each node will only contact an already contacted node if 20 s have passed. The pseudonym pool length p is set to 1 week, the slot length to 10 min. Cars are considered to be eligible for exchange of the current pseudonym, or candidates, when their speed difference is at most 10 km h^{-1}, the difference in heading is at most 15°, and their distance is no greater than 30 m. The beacon frequency does not affect the achieved level of privacy in our simulation as we used a stochastic attacker model. Based on findings in [3], we assume a strong attacker that follows pseudonym changes with a certainty of 95 percent. We simulated over 350 h of traffic with a total of over 1,500,000 cars until the margin of error was low enough. We evaluated the proposed scheme in a realistic urban scenario as well as in a synthetic four-lane freeway setup.

The urban scenario models traffic in the city of Ingolstadt, Germany. The road network itself was based on data by the OpenStreetMap project, adapted to reflect realistic intersection management. Traffic was created by randomly generating origin/destination pairs and iteratively applying dynamic user assignment, as implemented in SUMO, until the algorithm reported a stable, optimal distribution of flows. In the evaluation, we focus on the 4 km^2 region of interest (ROI), which contained a typical mix of high- and low-capacity roads, traffic lights, and unregulated intersections, as well as high- and low-density areas. To avoid border effects, traffic is simulated in the whole city of Ingolstadt, while the privacy scheme is only applied to nodes within the ROI.

To calculate the communication overhead caused by SlotSwap, we base the amount of data needed for pseudonym exchange on the proposed algorithms and certificate lengths in the upcoming WAVE standard. We assume a certificate length of 288 bytes with asymmetric key length of 1024 bits and symmetric key length of 128 bits for the *aes_128_ccm* scheme. From this, we conclude that the traffic needed for the exchange of a pseudonym, including IP overhead, is roughly 1 kbyte (i.e.,, 0.5 kbyte/node). Note that we neglect beacon messages in these calculations, since we consider them to be a prerequisite of ITS deployments in general, not of SlotSwap.

[1] *http://veins.car2x.org/*

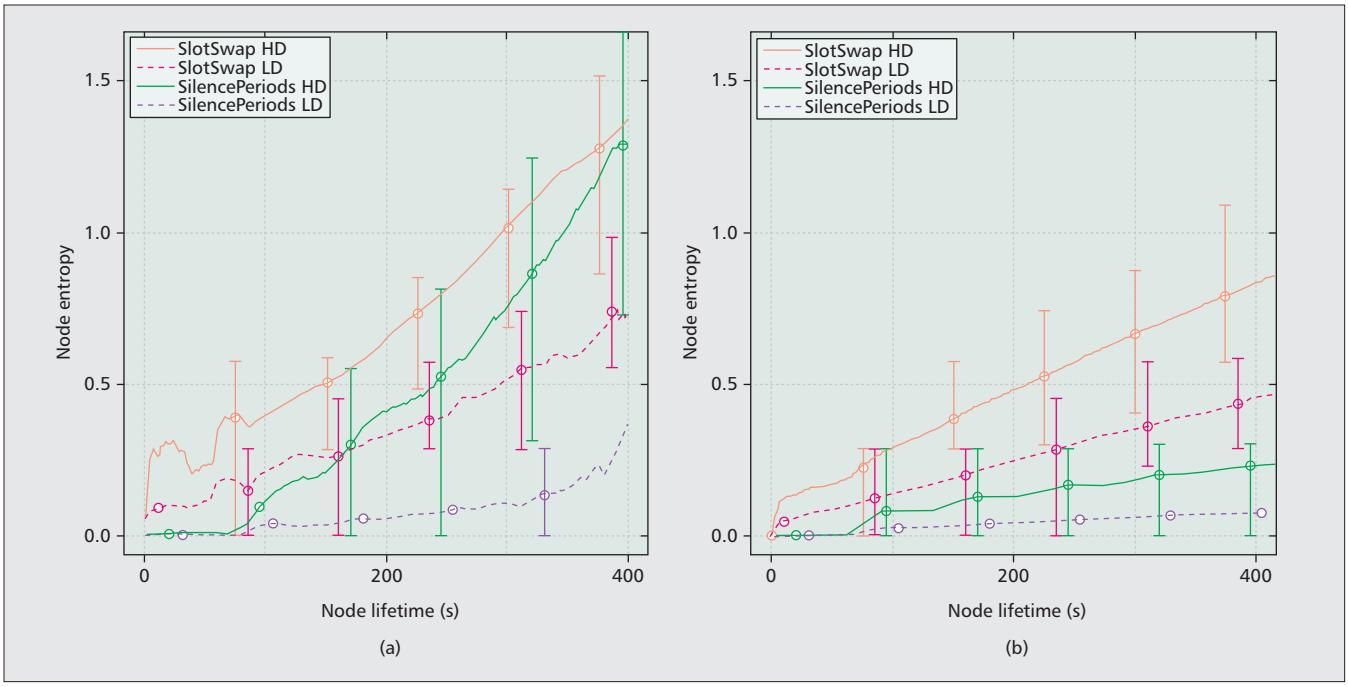

Figure 2. *Evaluation of the level of privacy as enjoyed by drivers in the ITS measured by means of the entropy: a) urban scenario; b) freeway scenario.*

Results

We compared SlotSwap with a mechanism that uses random pseudonym changes with subsequent silent periods, as still done in some field operational tests. A vehicle will randomly change its pseudonym and enter a random silent period of at most 10 s. The gain of location privacy is then dependent on nearby vehicles also being in such a random silent period.

Urban Scenario — The results for the simulation of the urban scenario are depicted in Fig. 2a. We observe nodes moving through the ROI, and calculate the entropy resulting from pseudonym exchanges and slot changes. We measured the mean level of privacy in a low-density (LD ≈ 16 cars/km^2) and a high-density (HD ≈ 100 cars/km^2) scenario.

In the urban scenarios the respective level of privacy achieved with SlotSwap was always higher than with random silent periods. It can be seen that in a low-density scenario, where location privacy is naturally harder to reach than in a high density environment, SlotSwap performs well compared to the random pseudonym change approach. While randomly changing pseudonyms depends on the coincidence of other vehicles being very close at the time of a pseudonym change, SlotSwap will systematically utilize such a situation by exchanging pseudonyms with the nearby vehicle.

As a result, drivers in SlotSwap will enjoy a higher level of privacy at the beginning of trips, while an initial delay is apparent for vehicles in order to become anonymous with the random change approach. As can be concluded from the second and third quartiles (illustrated by error bars), the number of vehicles that hold a considerably lower level of privacy relative to the mean entropy of all vehicles is higher when not using the SlotSwap system. These are vehicles driving on less frequented roads, hardly having a chance to become anonymous by randomly changing their pseudonym. As can be seen in the low density scenario, even after trip times longer than 350 s, more than 25 percent of all vehicles enjoy no location privacy at all, while cars using SlotSwap are clearly more anonymous.

The discontinuities at about 40 s and 90 s can be explained by the topology of our ROI. Two highly frequented roads cut the ROI. It took nodes about 40 s and 90 s, respectively, to pass these roads. The set of cars with these lifetimes therefore includes a considerable amount of cars with higher privacy levels, since on busy roads nodes will find potential partners for pseudonym exchanges more easily.

We measured the number of nodes suitable for exchange of the current pseudonym, the candidates of a node, according to our simulation setup parameters (speed difference ≤ 10 km/h, heading difference ≤ 15°, distance ≤ 30 m). As can be seen in Fig. 3a, in scenarios with densities ≤ 40 cars/km^2 most of the nodes are only very infrequently able to find one or more candidates. As expected, the number of candidates rises with the density. With 70 cars/km^2, 75 percent of all nodes frequently have one or more nodes suitable for pseudonym exchange nearby. The 5 percent quantile is still very low for the 100 cars/km^2 scenario, because there are always nodes traveling on infrequently used streets (e.g., in residential neighborhoods). It should be pointed out that even though finding a suitable node for pseudonym exchange was already very likely in higher-density scenarios, it will even be more likely in real-world scenarios, which frequently exhibit even higher node densities.

Figure 3b shows the number of exchanged future pseudonyms per minute, that is,

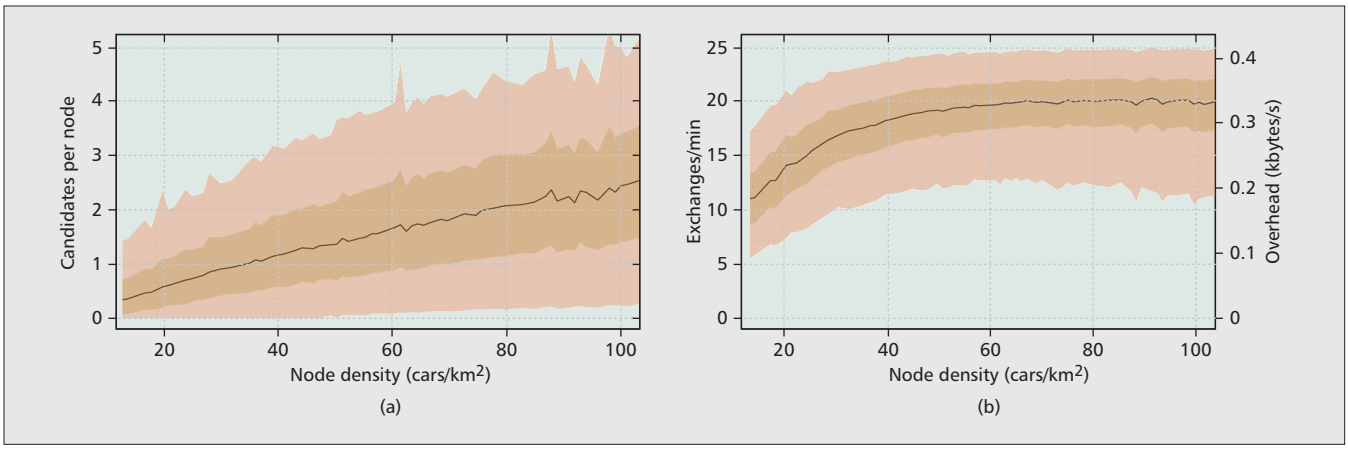

Figure 3. *Measurements for neighborship relations and resulting traffic overhead in the urban scenario. Overlaid are the 25 and 75 percent quartiles, and 5 and 95 percent quantiles, respectively: a) median candidates per node in the urban scenario; b) exchanges of future pseudonyms per node in the urban scenario with resulting traffic overhead.*

pseudonyms for slots other than the currently active one. One might expect that with higher density, the amount of pseudonym exchanges also rises. However, as can be seen, exchanges only marginally rise for scenarios with densities higher than 60 cars/km^2. The reasons for this are twofold. First, with more nodes in the network, the concurrency of nodes reacting to a beacon message will also increase. That is, new nodes not only offer more possibilities to exchange a pseudonym, but also compete for requesting exchanges from other nodes. Second, the more significant reason is that cars preferably exchange their current pseudonym rather than pseudonyms from other slots. With higher node densities, nodes will find suitable partners for exchanging their current identifier more easily, as shown in Fig. 3a. This also explains the slightly declining 5 percent quantile in higher-density scenarios. As expected, the traffic overhead caused by SlotSwap is insignificantly lower (Fig. 3b). It did not exceed an average of 0.5 kbytes s^{-1} and can therefore be deployed in an ITS without restriction.

Extrapolating our results, the observed pseudonym exchange rates meet a rate of 1200 pseudonyms/h. Assuming that, in a worst case scenario, traceable pseudonyms are only exchanged when the node carrying it initiates the pseudonym exchange, it would take less than 2 h to exchange the whole pseudonym pool. After this time period a node would only carry untraceable pseudonyms and already be completely anonymous when a new slot begins.

Freeway Scenario — In a second simulation run, we measured the location privacy enjoyed by vehicles on a four-lane freeway in both sparsely (LD ≈ 640 cars/h) and higher (HD ≈ 2160 cars/h) populated scenarios.

We found that on a freeway the entropy of nodes increases almost linearly with the lifetime of cars, as depicted in Fig. 2b. SlotSwap clearly outperforms the silent period approach. The cause for this is twofold: Vehicles almost immediately find a suitable candidate for pseudonym exchange on freeways. Second, the lack of intersections and high-density spots negatively influences the level of privacy reached by randomly changing pseudonyms. Even in the HD scenario, vehicles could not reach a similar level of privacy as with SlotSwap in the LD scenario.

Our findings suggest that after 10 min on a freeway, even in sparse scenarios with a strong attacker, vehicles implementing the SlotSwap scheme have reached a sufficient level of privacy.

Discussion and Research Challenges

We acknowledge that other cooperative privacy schemes that also utilize neighborship relationships will offer a similar degree of location privacy. In fact, an approach in which two nearby cars systematically change pseudonyms at the same time will be almost as effective as SlotSwap when it comes to complicating tracking for an overhearing adversary. Privacy mechanisms that further take group relations into account instead of only the relation between two vehicles can prevent tracking even more effectively. However, the key strength of SlotSwap is not necessarily the level of privacy obtained during a trip. It is rather the elimination of the mapping between base identity and pseudonym at the CA, and, by exchanging future pseudonyms, the anonymous start of a trip.

An open challenge in pseudonym exchange environments is the revocation of pseudonyms. If there is no mapping from a vehicle's base identity to all of its pseudonyms, revocation of the entire pseudonym pool of a vehicle is a nontrivial task. Another challenge is to make sure that no vehicle is able to harvest pseudonyms (i.e., to retain pseudonyms after transmitting them), thus threatening the safety and security of the whole system.

Conclusion

We present SlotSwap, a novel approach to increase the level of location privacy enjoyed by users in an ITS and eliminate the mapping between pseudonyms and base identities at a certificate authority (CA), thus protecting drivers in cases where the system provider is the attacker. We make use of a time-slotted

pseudonym pool, in which for every time slot there is exactly one pseudonym. By using this method, the workload at the CA is much less dependent on the number of nodes participating in the network, but rather on the rate of nodes joining it.

The synchronous change of identifiers increases the level of privacy of users that are close to other nodes in the network. To further increase anonymity and keep a CA from resolving pseudonyms to real identities of users, nodes exchange pseudonyms between one another. We show the general applicability of a novel concept for exchanging node identifiers in vehicular environments, having measured the resulting degree of privacy, using the entropy of nodes' anonymity sets.

Even when an adversary can track pseudonym changes with 95 percent certainty, our approach works well in both urban and freeway environments, and scales with the lifetime of a node in the network. Furthermore, the exchange of future pseudonyms makes it impossible for a central authority to resolve pseudonyms to identities even when a new time slot has just become active. We show that with very low communication overhead, nodes can exchange a sufficient amount of pseudonyms to swap all traceable pseudonyms for anonymous ones in short time periods.

References

[1] C. Sommer, O. K. Tonguz, and F. Dressler, "Traffic Information Systems: Efficient Message Dissemination via Adaptive Beaconing," *IEEE Commun. Mag.*, May 2011.

[2] P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," *7th Int'l. Conf. Pervasive Computing*, Nara, Japan, vol. LNCS 5538, Springer, May 2009, pp. 390–97.

[3] B. Wiedersheim *et al.*, "Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change is Not Enough," *7th IEEE/IFIP Conf. Wireless On Demand Network Sys. and Services*, Kranjska Gora, Slovenia, Feb. 2010.

[4] J.-P. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles," *IEEE Security and Privacy*, vol. 2, no. 3, May 2004, pp. 49–55.

[5] E. Schoch *et al.*, "Impact of Pseudonym Changes on Geographic Routing in VANETs," *3rd Euro. Wksp. Security and Privacy in Ad Hoc and Sensor Networks*, Hamburg, Germany, Sept. 2006.

[6] K. Sampigethaya *et al.*, "CARAVAN: Providing location privacy for VANET," *Embedded Security in Cars*, Tallinn, Estonia, July 2005.

[7] M. Li *et al.*, "Swing & Swap: User-Centric Approaches towards Maximizing Location Privacy," *5th ACM Wksp. Privacy in the Elect. Soc.*, Alexandria, VA, Oct. 2006, pp. 19–28.

[8] L. Huang *et al.*, "Enhancing Wireless Location Privacy Using Silent period," *IEEE WCNC '05*, New Orleans, LA, Mar. 2005.

[9] L. Fischer *et al.*, "Secure Revocable Anonymous Authenticated Inter-Vehicle Communication (SRAAC)," *4th Conf. Embedded Security in Cars*, Berlin, Germany, Nov. 2006.

[10] D. Eckhoff *et al.*, "Strong and Affordable Location Privacy in VANETs: Identity Diffusion Using Time-Slots and Swapping," *2nd IEEE Vehic. Net. Conf.*, Jersey City, NJ, Dec. 2010, pp. 174–81.

[11] M. Raya, R. Shokri, and J. Hubaux, "On the Tradeoff Between Trust and Privacy in Wireless Ad Hoc Networks," *Proc. 3rd ACM Conf. Wireless Network Security*, Hoboken, NJ, May 2010, pp. 75–80.

[12] M. Gerlach and F. Guttler, "Privacy in VANETs using Changing Pseudonyms — Ideal and Real," *IEEE Vehic. VTCSpring '07*, Dublin, Ireland, Apr. 2007, pp. 2521–25.

[13] Z. Ma, F. Kargl, and M. Weber, "Measuring Location Privacy in V2X Communication Systems with Accumulated Information," *6th IEEE Int'l. Conf. Mobile Ad Hoc and Sensor Sys.*, Macau SAR, China, Oct. 2009.

[14] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management — A Consolidated Proposal for Terminology," TU Dresden, TR v. 0.28, May 2006.

[15] A. Serjantov and G. Danezis, "Towards an Information Theoretic Metric for Anonymity," *2nd Int'l. Wksp. Privacy Enhancing Technologies*, San Francisco, CA, Apr. 2002, pp. 259–63.

[16] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Trans. Mobile Computing*, vol. 10, no. 1, Jan. 2011, pp. 3–15.

Biographies

DAVID ECKHOFF (de@cs.fau.de) received his M.Sc. in computer science (Dipl.-Inf. Univ.) from the University of Erlangen in July 2009 and is currently a Ph.D. student at the Chair for Computer Networks and Communication Systems. His research interests include privacy concerns in vehicular networks, ITS simulation, lower-layer modeling, and safety applications in Car-to-X environments.

CHRISTOPH SOMMER (christoph.sommer@uibk.ac.at) received his Ph.D. degree with distinction (Dr.-Ing.) and M.Sc. degree in computer science (Dipl.-Inf. Univ.) from the University of Erlangen in 2011 and 2006, respectively. In 2010, he was a visiting scholar with the Electrical and Computer Engineering Department of Carnegie Mellon University. Since 2011, he is a member of the ACM/Springer *Wireless Networks* editorial board. He is currently a postdoctoral researcher with the Computer and Communication Systems group at the University of Innsbruck. His research is focused on questions regarding efficiency and security aspects of Car-to-X communication in heterogeneous environments.

TOBIAS GANSEN (tobias.gansen@audi.de) received his diploma in communications engineering in 2004 from Wernigerode University of Applied Sciences, Germany. After working as a system analyst in the field of automotive research, he joined Audi electronics pre-development in 2007. Since then he has been involved in the evaluation and development of V2V and V2I communication systems (e.g., in the German field operational test simTD). His research interests are technologies for V2X security and privacy enhancement, with a focus on their industrial applicability.

REINHARD GERMAN (reinhard.german@cs.fau.de) received a diploma in computer science in 1991, his Ph.D. in 1994, and his Habilitation degree in 2000 from the Computer Science Department, Technical University of Berlin. Then he joined the Department of Computer Science at the University Erlangen-Nuremberg first as an associate professor (system simulation) and, since 2004, as a full professor (computer networks and communication systems) where he is currently head of the department. His research interests include model-based and measurement-based performance analysis, modeling and simulation paradigms and tools, numerical analysis of Markovian and non-Markovian models, vehicular communications, and autonomous sensor/actuator networks.

FALKO DRESSLER [SM] (falko.dressler@uibk.ac.at) is a full professor of computer science at the University of Innsbruck. He is an editor for journals such as Elsevier *Ad Hoc Networks*, ACM/Springer *Wireless Networks*, and Elsevier *Nano Communication Networks*. Among others, he wrote the textbook *Self-Organization in Sensor and Actor Networks* (Wiley, 2007). He is an IEEE Distinguished Lecturer in the fields of intervehicular communication, self-organization, and bio-inspired networking. He is a Senior Member of ACM (SIGMOBILE) and a member of GI (KuVS). His research activities are focused on adaptive wireless networking and self-organization methods addressing issues in wireless ad hoc and sensor networks, intervehicular communication systems, bio-inspired networking, and adaptive network security techniques.

We make use of a time-slotted pseudonym pool, in which for every time-slot there exists exactly one pseudonym. By using this method, the workload at the CA is much less dependent on the number of nodes participating in the network, but rather on the rate of nodes joining it.