


Article

Intelligent Adversary Placements for Privacy Evaluation in VANET

Ikjot Saini * , Benjamin St. Amour and Arunita Jaekel

School of Computer Science, University of Windsor, Windsor, ON N9B 3P4, Canada; stamourb@uwindsor.ca (B.S.A.); arunita@uwindsor.ca (A.J.)

* Correspondence: ikjot.saini@uwindsor.ca

Received: 16 July 2020; Accepted: 7 September 2020; Published: 14 September 2020



Abstract: Safety applications in Vehicular Ad-hoc Networks (VANETs) often require vehicles to share information such as current position, speed, and vehicle status on a regular basis. This information can be collected to obtain private information about vehicles/drivers, such as home or office locations and frequently visited places, creating serious privacy vulnerabilities. The use of pseudonyms, rather than actual vehicle IDs, can alleviate this problem and several different Pseudonym Management Techniques (PMTs) have been proposed in the literature. These PMTs are typically evaluated assuming a random placement of attacking stations. However, an adversary can utilize knowledge of traffic patterns and PMTs to place eavesdropping stations in a more targeted manner, leading to an increased tracking success rate. In this paper, we propose two new adversary placement strategies and study the impact of intelligent adversary placement on tracking success using different PMTs. The results indicate that targeted placement of attacking stations, based on traffic patterns, road type, and knowledge of PMT used, can significantly increase tracking success. Therefore, it is important to take this into consideration when developing PMTs that can protect vehicle privacy even in the presence of targeted placement techniques.

Keywords: location privacy; attack modeling; V2V communication; DSRC; vehicle-to-everything

1. Introduction

A Vehicular Ad-hoc Network (VANET) [1] consists of a network of vehicles and associated infrastructure that exchange relevant information, such as vehicle positions and status conditions, traffic density, and road conditions to improve road safety, reduce traffic congestion, and provide a variety of additional services to users. Safety applications require the exchange of valuable information about their status with other neighboring vehicles. This information includes its current location, speed, acceleration, steering angle, brake status, and a variety of other parameters. This information must be communicated in real-time, with minimum delay and frequent updates. Short to medium range wireless communication known as Dedicated Short Range Communication (DSRC) has been proposed to accommodate such Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications for safety-critical applications. Each vehicle broadcasts its relevant status information in the form of Basic Safety Messages (BSMs), using the IEEE 1609 DSRC/WAVE protocol stack [2], built on the IEEE 802.11p [3]. Based on the SAE J2735 standard [4], BSMs containing vehicle data such as location, speed, heading, and acceleration are sent multiple times per second and are not encrypted in order to reduce computational overhead for real-time processing. However, anyone within a vehicle's transmission range can receive BSMs from that vehicle and can use the information in successive messages to build a history of previous locations of the vehicle. Such tracking can be used to gather important information about the vehicle or drivers, including frequently visited places such as home or office location, visits to and from medical facilities or other sensitive areas and driving schedules.

Long term access to such information can compromise the location privacy of the vehicle users [5]. The concept of location privacy has been defined in the literature as “a special type of information privacy, which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others” [6]. Protecting location privacy is one of the leading security challenges in VANET communications [7]. One widely accepted approach for addressing the issue of location privacy is for vehicles to use pseudonyms instead of their actual ID, when communicating with neighboring vehicles [8]. A pseudonym is a temporary identifier issued by a trusted authority. The pseudonym certificates are typically attached to safety messages sent from a vehicle. The On-Board Unit (OBU) of an enrolled vehicle is responsible for vehicular communication and it receives multiple pseudonym certificates from the registration authority. A vehicle is assigned a number of pseudonyms but only one pseudonym (and corresponding certificate) is valid at a time. The pseudonym changing schemes considered in this paper use the 1609.2 standard [9].

Although pseudonyms make vehicle tracking more difficult, they are only effective if the pseudonyms are changed frequently. If the same pseudonym is used for an extended duration, an attacker may be able to deduce the vehicle identity based on driving history, trip start, destination points, etc. Additionally, even if the pseudonym is changed frequently, the changes should be implemented in a way that prohibits attackers from linking two (or more) pseudonyms associated with the same vehicle. The development of effective PMTs has become an important area of research in recent years and several approaches have been proposed [10–12]. Although different PMTs are available in the literature, they are typically evaluated with simplistic, randomly placed attackers and there is little or no information on the relative performance of these approaches under different conditions. In this paper, we propose two traffic-aware attacker placement strategies that can be used to select the most advantageous eavesdropping locations for attacking stations. To the best of our knowledge, this is the first work that considers intelligent placement strategies to cover the maximum number of vehicles with a limited number of attacking stations. We show how intelligent attacker placements can affect the performance of different PMTs and analyze the conditions under which privacy is most likely to be compromised. The main contributions of this paper are:

- A distance-based attacker placement scheme (DBAP).
- A novel speed-based attacker placement scheme (SBAP).
- A comprehensive comparative evaluation of different PMTs using the proposed schemes and random attacker placement, for different traffic conditions, using common metrics.

The two placement algorithms use prior knowledge of traffic patterns, road topology, and PMTs to locate attacking stations. This will provide a more realistic framework for evaluating both existing PMTs and those that may be developed in the future. The comprehensive comparison of current PMTs provide insights on their relative strengths and weaknesses, which can help determine the conditions under which each one can be used most effectively.

The remainder of the paper is organized as follows. In Section 2, we examine the current state of privacy management in VANET and some of the latest privacy schemes proposed in the literature. In Section 3, we describe our network model, as well as the adversary models and attacking methodology. In Section 4, we present two new attacker placement strategies that are based on distance and speed. Section 5 discusses the simulation setup and privacy metrics. In Section 6, the simulation results are presented and discussed and finally, we conclude our work in Section 7.

2. Privacy Management Techniques in VANET

The first step for protecting privacy in VANET is to dissociate the vehicle identity from the information trail to preserve privacy. As mentioned earlier, this is typically accomplished using a temporary ID called a pseudonym, which replaces the real vehicle identifier with a temporary random number. The Security Credential Management System (SCMS) [13] manages all the credentials and identities of authorized vehicles. The real identification and the associated temporary identifiers of

the vehicle are only revealed to designated participants of the communication network under special circumstances, e.g., when the vehicle is involved in malicious activity.

It is essential to change these temporary identifiers associated with a vehicle from time to time, in order to disconnect the information stream associated with an identifier. Many different PMTs that determine when and how often pseudonyms should be changed to improve privacy have been proposed in the literature [14–21].

The current PMTs can be categorized as area-oriented or user-oriented. Area-oriented approaches leverage the region of interest, often called mix zones [10,12,22], such as intersections, parking lots, or gas stations, which allow vehicles to change their pseudonyms with many other neighboring vehicles. However, area-oriented PMTs are prone to privacy attacks, as the adversary only needs to know the designated region(s) for pseudonym change. On the other hand, user-oriented PMTs do not rely on infrastructure or a particular area, which increases the uncertainty in terms of the locations where pseudonym change may occur. Therefore, in the remainder of this paper we will focus on user-oriented PMTs, which typically outperform other approaches.

The user-oriented PMTs use implicit triggers such as time [23], speed [14], neighboring vehicle density [15], or cooperation with other vehicles [16]. The periodic privacy scheme (PRD), introduced by Brecht et al. [13], has a static time-based trigger and is proposed as an element of the emerging standards by USDOT. The vehicle changes pseudonyms after every five minutes and selects a new pseudonym from a pool of twenty active pseudonyms, which is valid for one week. The size of the pool is restricted, so the pseudonyms allocated to a vehicle do not get exhausted too quickly. However, this often leads to reuse of pseudonyms, which makes it easier to link multiple pseudonyms.

In 2006, Li [11] introduced an approach with a dynamic speed-based trigger, which allows moving vehicles to swap their identifiers. However, there is an accountability problem in this scheme, and in 2009, Buttyan et al. proposed Silence at LOW speeds (SLOW) [14], another speed-based privacy scheme, where a pseudonym is changed when the speed of the vehicle drops below 30 km/h. The vehicle uses radio silence for a short period before changing its pseudonym. Since this is not based on a fixed place or time, it creates increased confusion for the adversary. However, using radio silence may have a negative impact on safety applications.

The anonymity of a vehicle is directly related to the number of other vehicles in its neighborhood. In 2009, Song et al. [15] introduced the first scheme with vehicular traffic-based triggers. Later, Pan proposed a Cooperative Pseudonym scheme based on number of Neighbors (CPN) [16] in which the vehicles require the cooperation of the nearby vehicles to simultaneously change pseudonyms. To increase anonymity, all the neighboring vehicles should change their pseudonyms at the same time. Benarous et al. [24] proposed a PMT that integrates two main factors: “hiding within the crowd” and “location obfuscation” techniques. The vehicle is forced to change pseudonym when either it is leaving specific geographical region or the pseudonym reaches its expiration. This PMT keeps count of neighboring vehicles and if the predefined neighbor threshold matches with current neighbors, then it cooperatively changes with other vehicles. Otherwise, the vehicle obfuscates its position and turns the speed to zero for the time the vehicle is changing its pseudonym. The drawback is that broadcasting inaccurate speed and position information raises concerns for the safety applications. The authors in [25] use reputation scores, sent as part of the periodic safety beacons, to trigger synchronous pseudonym changes, which increases the anonymity set. Liu et al. [26] presented another PMT which is fully uncoordinated and it aims to change pseudonyms in distributed networks to have frequent and unlinkable changes.

Context-based PMTs take into consideration the surrounding situation and change pseudonyms by adapting to the current situation. Context-Aware Pseudonym Scheme (CAPS) [17] is a context-aware scheme where the vehicle decides when to change the pseudonym based on surrounding conditions and keeps radio silence for a limited time prior to the change. Boualouache et al. [27] proposed a traffic-aware scheme, which needs congested areas for the pseudonym change and also uses radio silence. Context-based PMTs can be regarded as more intelligent, and the changes of the identifiers

are less likely to correlate to the target vehicles. CCAPS [28] is a combination of two previous PMTs (CPN and CAPS), which uses context awareness and cooperative strategy for changing pseudonyms. This PMT is user-oriented and the target vehicle keeps track of its neighboring vehicles. However, it uses radio silence in two out of three potential cases for changing pseudonyms. Zeng and Xu [29] proposed a mix context based Pseudonym Changing Privacy Preserving Authentication. Zhao et al. [30] presented a pseudonym changing game which was established by analyzing the relationship between pseudonym changing, cost, and privacy. Recently, a dynamic zone-based PMT [31] was proposed to establish an on-demand temporary swap zone, where a vehicle is able to randomly select and exchange the pseudonym with another vehicle without a group manager. This PMT adapts based on the surroundings to reduce the communication cost of forming pseudonym swap zones.

Table 1 shows the different triggers used by the PMTs discussed in this section. As the goal of this paper is to assess the effect of adversary placement on different PMTs, rather than introducing new PMTs, we have selected four promising user-centric PMTs for evaluation, as follows:

- Periodic [13],
- SLOW [14],
- CPN [16],
- CAPS [17].

Table 1. Pseudonym management techniques and triggers.

PMTs/Triggers	Time-Based	Speed-Based	Traffic-Based	Context-Based
Periodical [13]	✓			
SLOW [14]		✓		
Cooperative [16]			✓	
Dynamic Zone based [31]	✓			
Jaimes et al. [25]				✓
Liu et al. [26]			✓	
CAPS [17]				✓
Swing and Swap [11]		✓		
Song et al. [15]			✓	
Boualouache et al. [27]			✓	
CCAPS [28]			✓	✓
Mix-Context based [29]				✓
Zhao et al. [30]				✓
Benarous et al. [24]			✓	

The PMTs chosen (i) cover the range of different trigger metrics reported in the literature and (ii) represent the most well-established and widely used PMTs for comparisons. All the different PMTs listed in the literature review use one or more of the techniques from our selected list of PMTs. We note that the computation time of the different approaches for carrying out pseudonym change is very similar. The main difference lies in deciding when and under what conditions to initiate this pseudonym change.

3. Network and Adversary Model

When evaluating PMTs, it is important to consider both the network models and an accurate and realistic adversary model. In this section, we first discuss the network model and then our chosen adversary model as well as its tracking approach and capabilities.

3.1. Network Model

Our model considers that the vehicles are equipped with DSRC-enabled OBUs, which facilitate the Vehicle-to-Vehicle (V2V) as well as Vehicle-to-Infrastructure (V2I) communication. There are three main

entities, namely, Certificate Authority (CA), Roadside Unit (RSU), and OBU which communicate with each other. Figure 1 shows a diagram of our network model with the three levels of participating nodes.

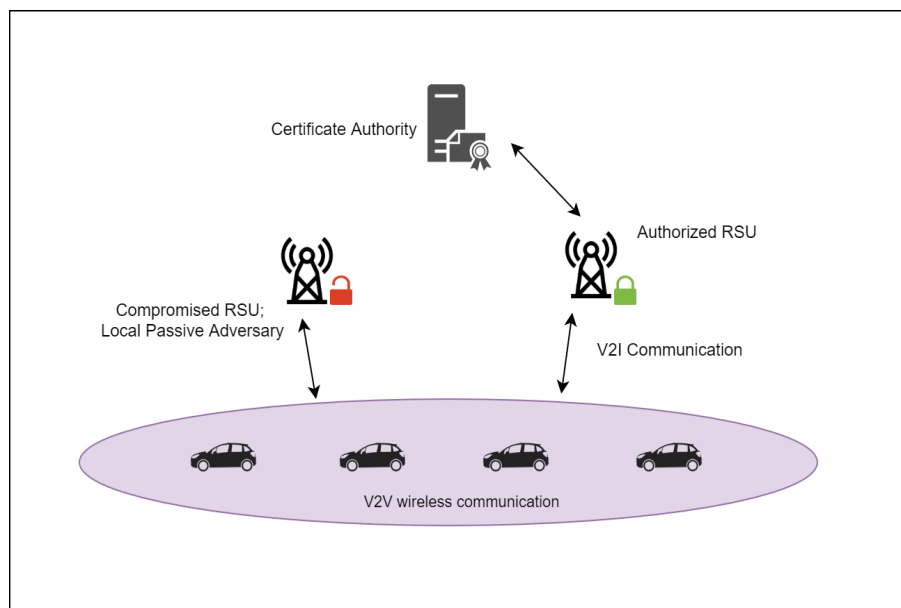


Figure 1. Network model.

CA in VANET is responsible for issuance of a set of a public and a private key to the participating vehicles and RSUs in the vehicular network. CA maintains the database for the long-term accountability of the registered vehicles by keeping a record of the original vehicle identification and the assigned pseudonym(s) along with the issuance time. In this paper, we assume the CAs are trusted entities. Approaches to deal with compromised CAs are available in the literature [32,33], but is out of the scope of this paper.

The DSRC-based RSUs are connected to each other as well as with the back-end CAs via a wired network. The RSUs can communicate timely information, such as road conditions and traffic incidents directly to vehicles and also receive BSMs sent by individual vehicles. If an RSU is compromised, it will be able to eavesdrop on all vehicles in its coverage area. We note that although compromised RSUs can behave as a local passive adversary, the attacker placements are not limited to just the RSU locations. They can be placed anywhere on the road network, and may or may not coincide with an RSU location.

The participating vehicle is equipped with an OBU which periodically broadcasts the situational awareness information to its immediate environment for safety applications. It has a Tamper-Proof Device (TPD) for securing sensitive information on the vehicle, such as credentials. The vehicle can participate in vehicular communication once CA authorizes the vehicle. Upon successful authorization, the vehicle enrolls with CA and obtains a pseudonym (or set of pseudonyms) signed by CA and timestamp(s) indicating the validity of the pseudonym(s).

3.2. Adversary Model

The active adversary typically aims to disrupt network communication, alter the information in the message or inject new messages into the network. The examples of such attacks are Man-in-the-Middle attack, timing attack, or broadcast tampering. The objective of the passive adversary, on the other hand, is to gain information to track and profile the drivers by eavesdropping on messages. This kind of adversary is passive as it does not modify messages or the message stream. Although the passive adversary typically does not disrupt the ongoing communications in the network, the main concern with this kind of attack is that it is very difficult to detect, because the adversary is simply listening to

the unencrypted messages and does not perform any alteration. In this paper, we focus on the passive adversary, whose primary goal is to compromise privacy of vehicles by linking pseudonyms.

The adversary can also be classified as global or local, based on the geographic area it can cover. The global adversary can eavesdrop on all the messages from all vehicles at all times, without leaving any blind spots. Many privacy evaluation schemes adopt this model, as it is the strongest adversary and can be used to model the “worst-case” situation. In a real-world scenario, this would require the adversary to place the equipment to cover a target geographic area, such as a city, completely. Considering the amount of equipment that would be needed to achieve this, the global adversary scenario is unlikely due to the prohibitive cost. Therefore, we have selected the local passive adversary model as an appropriate and realistic model for our simulations.

The local adversary only has access to a limited amount of attacking equipment, each with a specified communication range. Therefore, it is generally not able to eavesdrop on all vehicles in the area of interest. Due to the limitations on the number and communication range of the eavesdropping equipment, it is important for the local adversary to place these resources in a way that maximizes its attacking capabilities. The tracking approach we use is based on PREXT [34], which assumes global adversarial coverage, and we have redesigned the adversary according to our algorithms [35,36]. PREXT uses Multi-Hypothesis Tracking [37], which relies on Kalman Filter [38] and a multi-target tracking algorithm, Nearest Neighbor Probabilistic Data Association (NNPDA) [39], to track vehicles with anonymous message collection. If the pseudonym is changed, the vehicle tracker predicts the target vehicle based on the location and time information. It may accurately identify the target vehicle (successful tracking) or may observe it as a new vehicle or incorrectly associate it with a different vehicle (unsuccessful tracking).

Factors Affecting Tracking Ability

For the local passive adversary considered in this paper, several important factors can affect vehicle tracking, as identified below.

- The number of vehicles changing pseudonyms simultaneously: A vehicle changing its pseudonym alone is relatively easy to recognize. Therefore, PMTs, where multiple vehicles cooperate to change pseudonyms together, tend to perform better. This depends on (i) the choice of PMT being used and (ii) the vehicle density. We have considered both factors in our simulations.
- Knowledge of PMT and traffic analysis: If the PMT is known to the attacker, the attacker can exploit this knowledge to place the listening stations strategically. In addition, stations can be placed in high-traffic areas, if traffic patterns are known, to eavesdrop on more vehicles. Certain PMTs lead to the repetition of pseudonyms, which can also be exploited by the adversary. We have compared the proposed schemes, which exploit knowledge of PMT and traffic patterns, with random placement strategy to investigate this factor.
- Communication range of listening stations: Reducing the listening range of the attacking stations results in fewer BSMs reaching the eavesdropping stations and reduces successful vehicle tracking. We have considered different listening ranges to study the impact of this parameter on tracking success.

4. Intelligent Attacker Placement

In this section, we present two new attacker placement strategies—(i) distance-based attacker placement (DBAP) and (ii) speed-based attacker placement (SBAP) for selecting the locations where attacking stations should be placed to increase the chances of successful vehicle tracking. For both approaches, this is accomplished by selecting locations where

1. attacking stations can listen to beacons from many vehicles and
2. pseudonym changes are likely to occur.

The placement algorithms use knowledge of long term traffic patterns to help select potential locations for adversary placement. Such information can be easily obtained from public sources to retrieve real-time traffic information using a variety of web applications such as Google Maps [40], so the algorithms are not dependent on any specialized or proprietary data. The collected traffic information can include the most congested road segments or intersections, time of the day, the usual duration of congestion, and length of the road segments with congestion.

4.1. Distance-Based Attacker Placement

A brief overview of our proposed distance-based attacker placement (DBAP) algorithm is given below in Algorithm 1. In this approach, the attacker chooses specific road segments, based on traffic conditions and places attacking stations at specified distances along with the selected segments. DBAP scheme is designed to be effective against PMTs that use a static trigger, e.g., periodic. In such PMTs, pseudonym change is triggered at specific time intervals. Therefore, DBAP places attacking stations separated by a distance d , which is calculated based on several possible factors. For listening stations with communication range r_{comm} , setting $d \leq 2 \cdot r_{comm}$ on a particular road segment can achieve full coverage for that segment. However, due to limitations on the amount of available attacking stations, the spacing may need to be increased, which means some pseudonym changes may go unobserved.

First, we select a suitable target destination T (step 1a), which is likely to be visited by a large number of vehicles. For urban scenarios, T is typically a high-traffic road, often near the city center, while for highways, it is always taken as the last segment of the highway. Next we identify a set P of k potential starting points (step 1b), where $p_i \in P$ and $1 \leq i \leq k$. The road segments from p_i to T are selected for adversary placement. The goal is to select roads that have high traffic so that more vehicles will be exposed to attacking stations. For highways, $k = 1$ and p_1 is the initial segment of the highway under consideration. In other words, we do not consider the highway on or off-ramps, but rather treat it as a single road segment.

Algorithm 1 Distance-based attacking algorithm

Input: Amount of available equipment for tracking the vehicles (n) and PN change frequency (f)

Output: Adversary spacing

- 1: Based on traffic patterns select
 - a. Target destination (T)
 - b. a set P of potential starting points for routes, where $P = k$ and $p_i \in P$ is the i th starting point.
 - 2: Calculate spacing between adversary positions (d)
 - 3: Calculate lower limit $N_{min} = \sum_{i=1}^k \lceil \frac{dist(p_i, T)}{d} \rceil$ for number of adversaries to use.
 - 4: **if** $n < N_{min}$ **then**
 - 5: a. calculate d' , where d' is the smallest spacing for which $n \geq \sum_{i=1}^k \lceil \frac{dist(p_i, T)}{d'} \rceil$
 - 6: b. Set $d = d'$
 - 7: **end if**
 - 8: **for** $p_i \in P$ **do**
 - 9: Place adversary equipment with space d along route from p_i to T.
 - 10: **end for**
-

After selecting the routes, we determine the maximum distance (d) between successive attacking stations along the selected routes (step 2) in order to achieve full coverage along these routes. The value of d can depend on several factors, such as vehicle speeds, the frequency of pseudonym changes and the communication range of the attacking stations. Next, in step 3, we determine the minimum number of attacking stations (N_{min}) needed for covering the routes, based on d . If the number of available stations (n) is higher than N_{min} , then d is set to be the attacker distance. On the other hand, if $n \leq N_{min}$, we calculate an updated attacker spacing d' (step 4–7), where $d' > d$ and then set $d = d'$. It is important

to note that increasing the attacker spacing may have a negative impact on the ability to track vehicles. Finally, the stations are placed along each selected route with a distance of d between two adjacent stations (steps 8–9).

4.2. Speed-Based Attacker Placement

The DBAP scheme in the previous section works well for periodic pseudonym changes, but may not be effective for a speed-based PMT. In a speed-based PMT, the pseudonym changes when the speed falls below a given threshold, for example, at red light intersections and stop signs or along sections of roads that experience high traffic congestion. In the remainder of this paper, we refer to an intersection with a traffic light or stop sign as a Traffic/Stop Intersection (TSI) and congested road segments as High Traffic Sections (HTSs). TSIs and HTSs are excellent candidate locations for placing attackers when vehicles are using speed-based PMT. However, it might not be feasible to place attacking stations on all TSI or very closely spaced along with an HTS. The SBAP algorithm given below identifies potential attacker positions so that more vehicles can be tracked with relatively few attacking stations. The speed-based attacker placement (SBAP) scheme is designed to be effective against PMTs that use a speed trigger, e.g., SLOW. In such PMTs, pseudonym change is triggered when the vehicle speed falls below a specified threshold. Therefore, SBAP places attacking stations at or near locations where vehicle speed is likely to be low, such as intersections with traffic lights or stop signs or along road segments that generally have high traffic congestion, based on long term traffic patterns. Monitoring a longer stretch of the road helps in the correlation of the old and new pseudonyms of a vehicle. Therefore, we consider segments that are relatively long (at least 15 km) and have high traffic density.

An overview of our proposed speed-based attacker placement is given in Algorithm 2. Based on the long term traffic patterns, two types of road segments are selected for monitoring:

- A set $S1$ of urban road segments where attackers will be placed based on TSI locations, where $S1 = k$ and $s_i \in S$ is the i th road segment and
- a set $S2$ of road segments (primarily highways, but may contain some urban roads as well), where attackers will be placed based on traffic congestion.

Algorithm 2 Speed-based attacking algorithm

Input: Number (n) and communication range (r_{comm}) of available attacking stations for vehicle tracking

Output: Adversary locations

- 1: Repeat steps 2–15 until all selected locations are covered or there is no more available attacker equipment
 - 2: **for** $s_i \in S1$ **do**
 - 3: loc_A = location of the first TSI of s_i
 - 4: Repeat steps 5–8 until $loc_A \in s_i == \text{False}$:
 - 5: Place attacker at loc_A
 - 6: d_{next} = distance from loc_A to the next TSI on s_i after loc_A
 - 7: $d_{inter} = \max\{d_{next}, 2 \cdot r_{comm}\}$
 - 8: $loc_A = loc_A + d_{inter}$
 - 9: **end for**
 - 10: **for** $HTS_i \in S2$ **do**
 - 11: loc_A = location of first attacker in HTS_i
 - 12: Repeat 13–14 until $loc_A \in HTS_i == \text{False}$
 - 13: Place attacker at loc_A
 - 14: $loc_A = loc_A + 2 \cdot r_{comm}$
 - 15: **end for**
-

Attacking stations are placed one by one on the selected road segments, based on TSI (steps 2–9) and HTS (steps 10–15), until all positions of interest have been covered or the maximum number of stations (n) have been used. For each selected road segment s_i on an urban road, the current attacker location is initially set to the first TSI of the segment (step 3). If the specified attacker location (loc_A) falls within the current road segment s_i , (step 4) then attacking equipment is placed at loc_A (step 5). Once the equipment has been placed, steps 6–8 determine the next location to be used for placing additional equipment on the current segment. If the distance from the current TSI to the next one is greater than $2 \cdot r_{comm}$, then an attacker is placed at the next TSI. Otherwise, next attacker is placed at a location $2 \cdot r_{comm}$ from the current TSI on the road segment s_i . This placement strategy allows all the TSIs along the road segment to be covered using the fewest possible attackers.

Once attackers have been placed at intersections, we try to place any additional equipment along with congested road segments, i.e., $HTS_i \in S2$ (steps 10–14). The first attacker along an HTS is placed at a location that is at a distance of $2 \cdot r_{comm}$ from the nearest station. Subsequently, equipment is placed uniformly at intervals of $2 \cdot r_{comm}$ along the entire segment.

5. Simulation and Analysis

For our simulation study, we have used the Vehicles In Network Simulation (VEINS) [41] framework, which allows bi-directional coupling of the network simulator with the road traffic simulation. The network simulation is carried out using OMNET++ [42] along with Simulation of Urban MObility (SUMO) [43]. OMNET++ is a discrete event simulator for the communication network which simulates the components and modules based on the defined communication stack. For privacy evaluation, we used PREXT [34], which enables the comparison of different schemes with each other based on the same privacy metric. For the urban scenarios, we considered a 6500 m by 6500 m area in the city of London, Ontario, while for the highway scenarios, we considered a 26,000 m by 11,000 m area on the outskirts of London, Ontario. In both cases, OpenStreetMap [44] was used to obtain realistic geographical map files. The urban setting has complex road topology, with intersections where direction of travel may change. For the highway scenario, the vehicles follow a specific direction for a longer duration. Therefore, vehicle routes are more predictable, as the vehicles do not have many options to change the trajectory except at an exit point. Figures 2 and 3 show the locations of the attackers (assuming 3 attacking stations), using the different placements strategies for urban and highway scenarios, respectively. These placements were used for all the simulations discussed in this section.



Figure 2. Attacker locations in highway scenario.

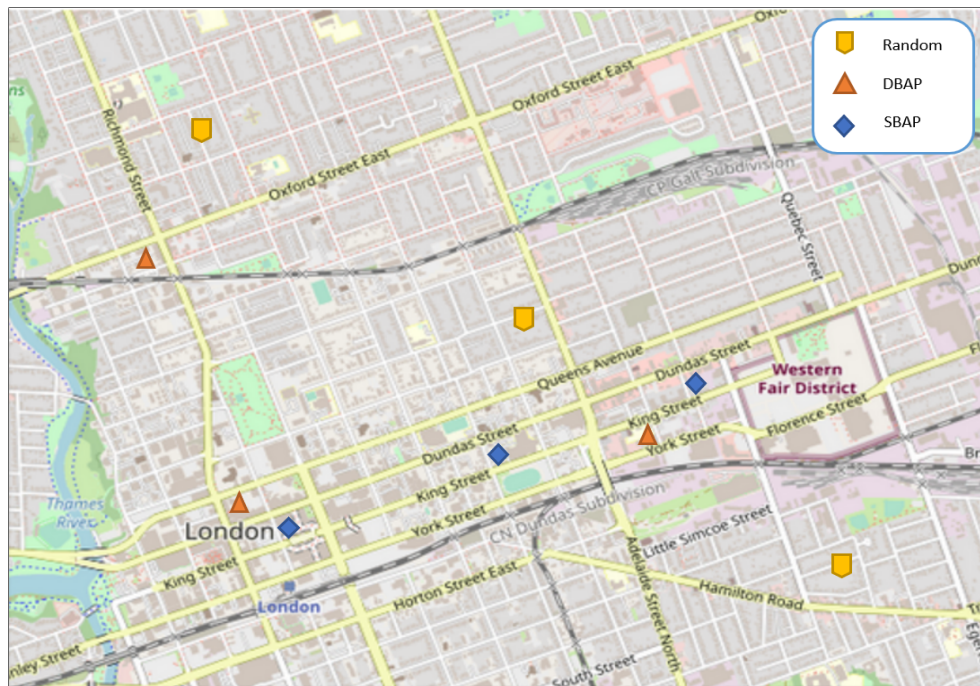


Figure 3. Attacker locations in urban scenario.

We evaluated the effect of adversary placement on different PMTs, under different traffic conditions, attacker capabilities, and eavesdropping durations. The relevant simulation parameters are listed below:

- Adversary model: Local passive adversary.
- PMT approach: Periodic [13], SLOW [14], CPN [16] and CAPS [17].
- Placement scheme: Random, DBAP, and SBAP.
- Road type: Urban or highway.
- Vehicle densities: 100, 200, and 300 vehicles.
- Number of attacking stations: 3.
- Listening range of attacking stations: 500 m, 700 m and 1000 m.
- Eavesdropping duration: 300 s.

To have the evaluation with the highest possible eavesdropping capabilities, we assume that there is a minimum effect of the obstacle shadowing caused by the building and infrastructures. We considered that the eavesdropper receives the safety messages within its listening range without any significant packet loss. To obtain a realistic vehicle movement, we have used random trip generation for urban traffic, which initializes the vehicles from different origins and assigns routes to distinct destinations.

Performance Metrics

Different metrics can be used to evaluate the performance of the PMTs. In this paper, we define two metrics, the tracking success rate (TSR) and global tracking success rate (GTSR), to measure how well vehicles can be tracked while using various PMTs. These metrics are from the adversary's point of view, so a higher value of TSR or GTSR is better for the adversary but could point to a potential weakness in the PMT. We use the following notation to define our metrics:

- V : Set of all vehicles in the simulation.
- N_v : Total number of vehicles in the simulation, i.e., $N_v = V$.
- N_a : Total number of vehicles that come within the listening range of at least one attacking station. We note that for a global adversary $N_a = N_v$, while for a local adversary $N_a \leq N_v$.
- PN_v : Set of distinct pseudonyms used by vehicle $v \in V$ over a complete trip from source to destination.
- c_v : Number of pseudonyms changes carried out by vehicle $v \in V$ over a complete trip from source to destination.
- $PN_{v,i}$: Specific pseudonym in use by vehicle $v \in V$ after the i th pseudonym change $1 \leq i \leq c_v$. $PN_{v,0}$ corresponds to the initial pseudonym used by vehicle v . We note that if a vehicle v does not repeat any pseudonyms over its entire trip, then $PN_v = c_v + 1$; however if pseudonyms are repeated then $PN_v \leq c_v$.

For a vehicle $v \in V$ undergoing a pseudonym change from $PN_{v,i}$ to $PN_{v,i+1}$, we consider the pseudonym change event to be tracked successfully if both the old and new pseudonyms are associated with the same vehicle by the adversary. On the other hand, an unsuccessful tracking event for vehicle v occurs if (i) two pseudonyms used by vehicle v are not recognized as belonging to the same vehicle by the adversary or (ii) a pseudonym belonging to a different vehicle is linked to vehicle v by the adversary.

We set $s_v = 1$ if a vehicle v is successfully tracked over its entire trip, i.e., if following conditions are both satisfied.

- There is a total of c_v successful tracking events associated with v and
- there are no unsuccessful tracking events associated with v .

Based on the above definitions, we calculate the overall tracking success rate for a simulation run as

$$TSR = \frac{\sum_{v \in N_a} s_v}{N_a} \cdot 100 \quad (1)$$

Similarly, we calculate the overall global tracking success rate for a simulation run as

$$GTSR = \frac{\sum_{v \in N_a} s_v}{N_v} \cdot 100 \quad (2)$$

We note that the impact of the intelligent placement strategies is expected to be reflected in terms of higher GTSR values (but not necessarily higher TSR) when using such schemes.

This is because when listening stations are in areas with low vehicle density, it may be easier to track the limited number of vehicles in its range since fewer vehicles cause less confusion; however overall only a small percentage of vehicles are actually being eavesdropped.

6. Results

There are several factors such as vehicle density, listening range of attacking stations, and the PMT and placement strategy being used that influence how successfully vehicles are tracked. In this section, we consider the impact of these factors and discuss and analyze the results of our simulations. The graphs included in this section show average values, along with the the 95% confidence intervals for these values.

6.1. Number of Eavesdropped Vehicles

The objective of the placement strategies presented in this paper was to increase the number of “eavesdropped” vehicles, i.e., the set of vehicles (N_a) that come within the listening range of at least one attacking station. Figure 4 compares the number of eavesdropped vehicles for different placement schemes. We see that both DBAP and SBAP significantly improve (by at least double) the chances

that a vehicle will be eavesdropped. The performance of DBAP and SBAP are similar for the urban scenario, while SBAP performs better in highways.

6.2. Results for the Base Case

We selected a standard set of parameters to observe “base case” performance of each PMT and placement scheme and then varied these to observe their effect on the tracking ability of the adversary. For the base case, we simulated for 300 s with a vehicle density of 200 in the presence of 3 eavesdropping stations with a 500 m listening range. The performance is measured in terms of the tracking success rate (TSR) and global tracking success rate (GTSR).

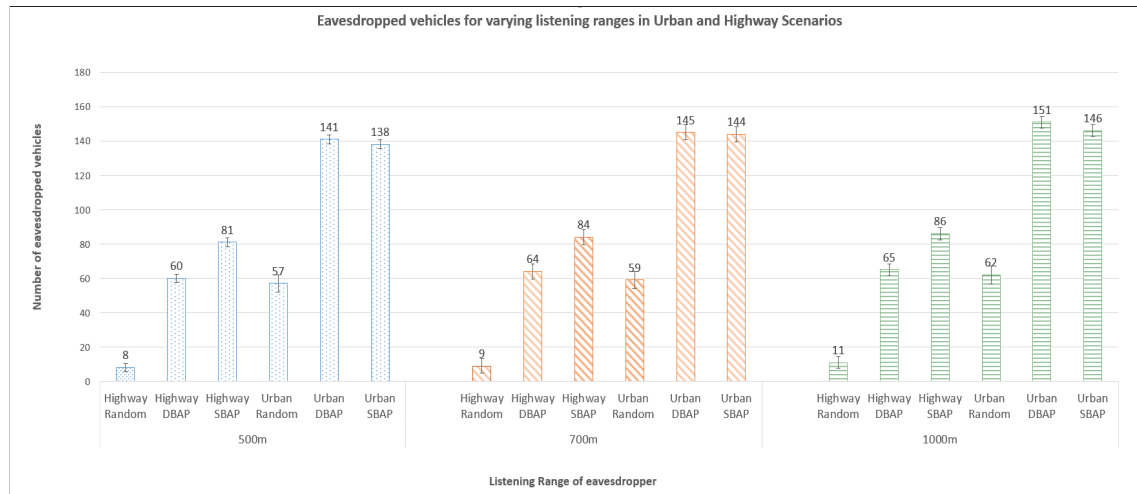


Figure 4. Comparison of eavesdropped vehicles for varying listening ranges in different scenarios.

Figure 5 shows the GTSR values for highway traffic using different PMTs for random, DBAP, and SBAP placement schemes, respectively. The performance of the PMT depends on placement schemes, based on their triggers and frequency of pseudonym change. This means that if the adversary is aware of the PMT being used, this information can be exploited to use the placement strategy that has the highest GTSR for that PMT.

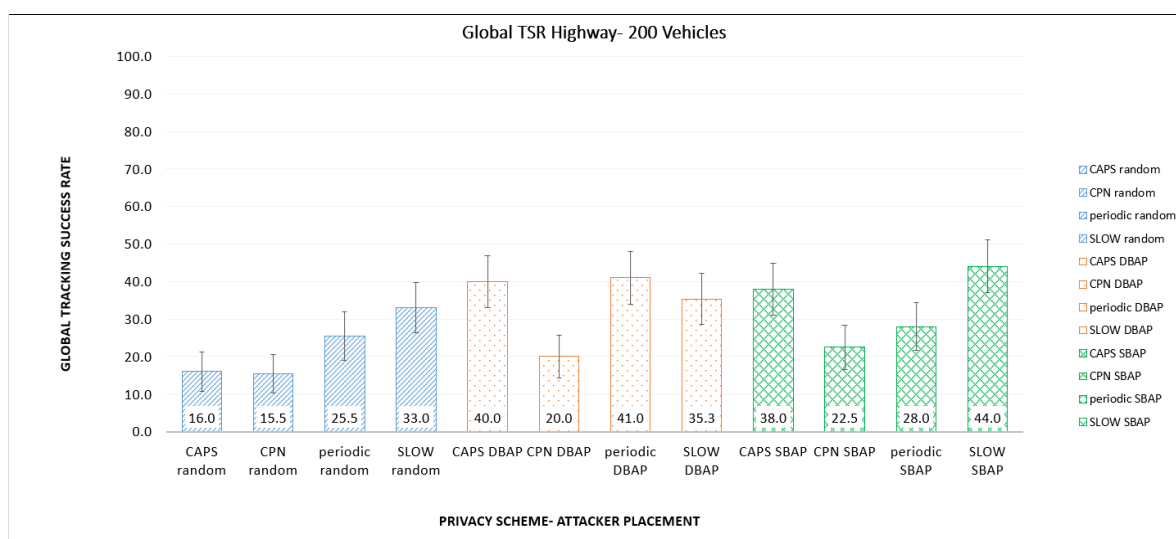


Figure 5. Comparison of global tracking success rate (TSR) for different placements and Pseudonym Management Techniques (PMTs) in the highway scenario.

The average GTSR over all PMT approaches for DBAP and SBAP are very similar (34% and 33%, respectively), as opposed to random placement, which is only 22.5%. Furthermore, regardless of the PMT being used, random placement always has a lower GTSR, compared to both DBAP and SBAP. This shows that with limited resources, the strategic and intelligent placement of the eavesdropping stations can result in an increased rate of successful tracking. It is important to note that for highway scenarios, three adversary stations with a listening range of 500 m cover only a small fraction of the region of interest (26,000 m \times 11,000 m) and can still achieve an overall successful tracking percentage of more than 30%.

When comparing the different PMTs, we noted that the cooperative approach (CPN) seems to work uniformly well (i.e., lower GTSR values) across the different placement schemes. The performance of the other PMTs varied significantly based on the attacker placement. For example, SLOW; which uses a speed trigger, performed the worst for speed-based placement (SBAP); and the periodic scheme performed the worst with DBAP placement, which targets this scheme.

Figure 6 shows the corresponding GTSR values for the base case, for urban traffic. The relative performance of the PMTs is very similar to that for highway traffic, although there is some slight variation in the actual values. For random placement, we observed no significant differences between the highway and urban traffic. For DBAP with urban traffic, slightly more vehicles were tracked for periodic PMT and fewer for CAPS. Similarly, for SBAP, GTSR value increased for SLOW, this could be attributed to more vehicles changing their pseudonyms near the attacking stations, due to the lower speeds in urban environment.

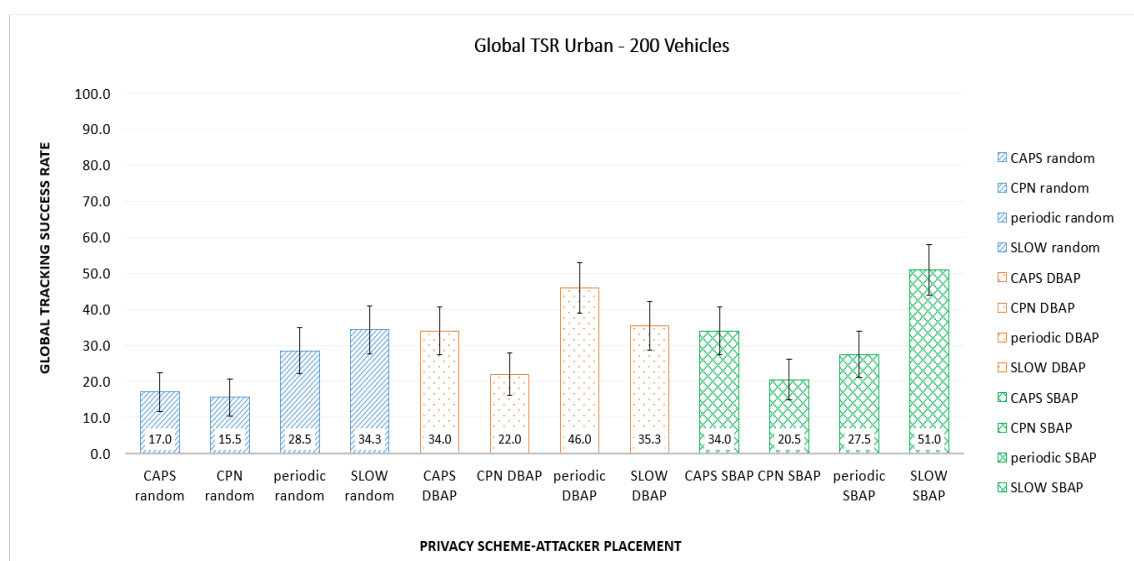


Figure 6. Comparison of global TSR for different placements and PMTs in the urban scenario.

Figures 7 and 8 show the TSR values for different privacy approaches and placement schemes for highway and urban traffic. The TSR values are significantly higher compared to GTSR since they do not consider vehicles that are out of range of the eavesdropping stations. For example, for highway traffic, the GTSR values for SLOW range from 33–44%, while the corresponding values for TSR are 85–94%, and for CPN using DBAP, the TSR is 100%. It is interesting to note that there appears to be no clear correlation between the placement scheme and TSR. For example, in several cases, random placement results in higher TSR compared to the more informed schemes like DBAP or SBAP. Both of these observations can be explained by the fact that TSR calculations ignore all vehicles that are not ‘observed’ by any listening station. This means that if a listening station is in an area with very few vehicles, it will likely be able to successfully track those vehicles since fewer vehicles mean less confusion for the attacker. This will lead to a higher TSR, even though many vehicles are not being observed at all. In such cases, random placement will produce a higher TSR as the other approaches

always try to put stations in the most congested locations. It can also lead to a TSR of 100% if very few vehicles appear within the listening range of the stations, leading to easier tracking.

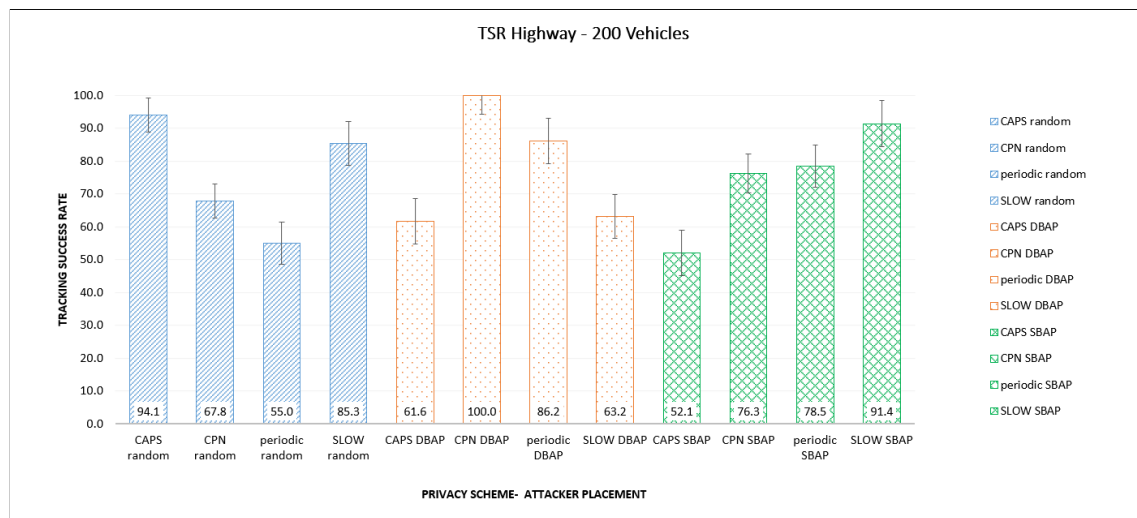


Figure 7. Comparison of TSR for different placements and PMTs in the highway scenario.

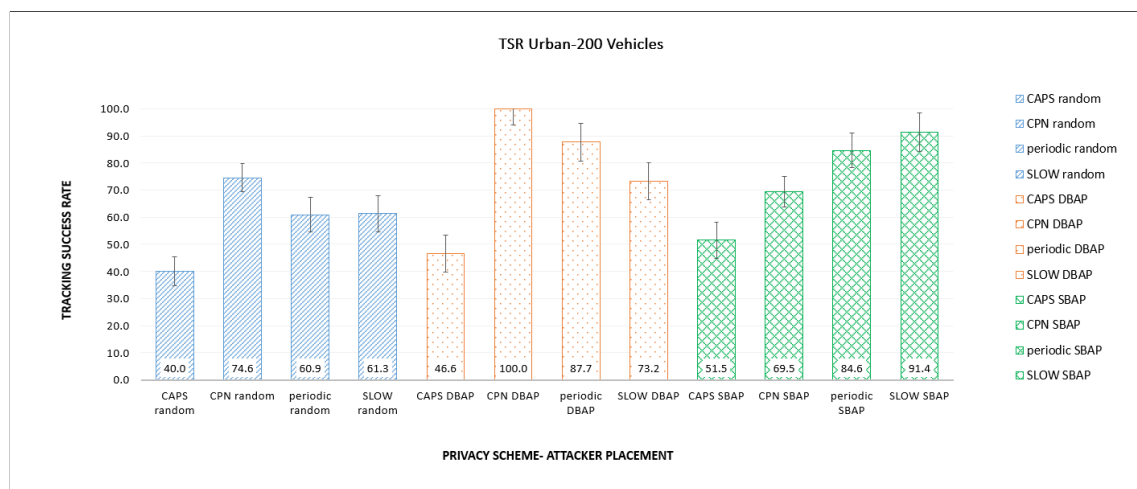


Figure 8. Comparison of TSR for different placements and PMTs in the urban scenario.

The vehicle speed can potentially affect the tracking performance, and the degree of impact (if any) depends heavily on the specific PMT and the placement strategy being used. In our simulations, we have considered both urban and highway scenarios, with different vehicle speeds of 50 km/h and 100 km/h, respectively. In most cases, vehicle speed did not have a significant impact. However, based on our observations, the effect of vehicle speed was evident when a speed-triggered PMT (SLOW) was used along with SBAP. In this case the urban scenario (which has lower vehicle speeds) showed an increased global tracking success rate (GTSR). We expect this will be the case with other speed-based PMTs as well, while PMTs with non-speed triggers would not be highly impacted by vehicle speed.

6.3. Vehicle Density

Tables 2 and 3 show the performance of the different PMTs for different vehicle densities on the road network, for urban and highway scenarios, respectively. Overall, the results indicate that the tracking success rates for the proposed placement strategies, SBAP and DBAP, are consistently similar to or higher than random placement. Both the highway and urban scenarios followed a similar trend, with some small variations in the actual values. We also noted that the effect of vehicle density seemed

to depend heavily on both the PMT and placement strategy being used. Therefore, we give a brief description of how vehicle density affects GTSR for the different approaches below.

Table 2. Urban scenario: Effect of vehicle density on GTSR.

Number of Vehicles	Random				DBAP				SBAP			
	CAPS	CPN	PRD	SLOW	CAPS	CPN	PRD	SLOW	CAPS	CPN	PRD	SLOW
100	17	20	30.5	11.3	25	48	45.5	32.7	25	20	38.5	45.7
200	17	15.5	28.5	34.3	34	22	46	35.3	34	20.5	27.5	51
300	30	15.5	11.3	34.7	48	17	47	25.3	39	17.5	27	51.3

Table 3. Highway scenario: Effect of vehicle density on GTSR.

Number of Vehicles	Random				DBAP				SBAP			
	CAPS	CPN	PRD	SLOW	CAPS	CPN	PRD	SLOW	CAPS	CPN	PRD	SLOW
100	16	18	33	11	24	46.5	42.5	36	24	25	36	49.33
200	16	15.5	25.5	33	40	20	41	35.3	38	22.5	28	44
300	37	15.5	10.7	33.7	54	18	47	25.7	38	21	25.3	43.3

The context-aware scheme (CAPS) shows the highest tracking rate of 48% in the presence of 300 vehicles with a DBAP placement strategy and the least with random placement with a tracking rate of 17%. For the proposed placement strategies, GTSR increases with number of vehicles, as more pseudonym changes will occur in high density areas, where attacking stations are placed. Therefore, pseudonym changes are more likely to take place within the listening range of the stations. The cooperative scheme (CPN) has the highest tracking rate of 48% in the presence of 100 vehicles with a DBAP strategy. The GTSR decreases as the vehicle density increases because this scheme triggers a massive number of pseudonym changes as the number of vehicles increase, making it difficult to track the vehicles. In our mobility model using random trips, many of the vehicles were out of the observation of the eavesdropping station, causing an overall decline in the tracking rate. This effect was particularly evident for DBAP placement. For the periodic scheme, the best placement strategy is DBAP, as it has the highest overall GTSR regardless of the number of vehicles. For SBAP and random placement, tracking success decreases slightly with higher vehicle density as a higher number of vehicles can lead to more confusion for the attacker. SBAP has the highest tracking rates (35–51%) for the SLOW scheme, and the tracking success rate varies only slightly with number of vehicles. The GTSR for DBAP (25–36%) and random placement (11–35%) are consistently lower since they do not allow the tracker to strategically cover high traffic areas or the areas with potential traffic jams. With DBAP, GTSR does not seem to correlate strongly with number of vehicles, while it increases with vehicular density for random placement.

Some important observations, based on our simulations, are summarized below.

1. Different PMTs have different vulnerabilities and these can be exploited by the adversary by placing eavesdropping stations accordingly if the PMT being used is known.
2. Intelligent adversary placement consistently results in more vehicles being eavesdropped and consequently higher tracking success rates by the adversary, compared to random placement.
3. The effect of vehicle speed and vehicle density depend heavily on the PMT and the placement scheme being used. For example, SBAP is very effective with SLOW (which uses a speed-based trigger), since it was designed to target such PMTs.

7. Conclusions

In this paper, we proposed two intelligent adversary placement strategies (DBAP and SBAP) for locating eavesdropping stations along vehicle routes, based on traffic density, road type, and knowledge of the pseudonym technique used. We have shown that using the proposed placement schemes, it is possible to track more vehicles compared to a random placement strategy, which is typically used for evaluation. This demonstrates the need to take into consideration the impact of targeted attacker placement schemes when evaluating different PMTs. We have also studied four well-known PMTs and assessed their performance under urban and highway traffic for various placement schemes, traffic densities, and attacker capabilities. This shows how weaknesses of a selected scheme can be exploited by an intelligent attacker to track more vehicles successfully. The insights gained from this study will be used to develop a comprehensive pseudonym changing framework that can be effective for a wide range of different traffic conditions and attacking scenarios. Some potential strategies to mitigate the vulnerabilities of the existing PMTs could be (a) have multiple nearby vehicles with similar speeds change pseudonyms simultaneously and (b) for time-based triggers, make sure intervals are unpredictable rather than constant.

Author Contributions: I.S., A.J. were responsible for conceptualization of the paper. B.S.A. extended the software and collected the data. I.S. developed the software framework, performed analysis and validation, and wrote the paper under the supervision of A.J. A.J. supervised the research and provided guidance and key suggestions in writing the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by NSERC DG, Grant # RGPIN-2015-05641.

Acknowledgments: The work of A. Jaekel has been supported by a research grant from the Natural Sciences and Engineering Research Council of Canada (NSERC).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BSM	Basic Safety Message
CAPS	Context-Aware Pseudonym Scheme
CPN	Cooperative Pseudonym scheme based on number of Neighbors
DSRC	Dedicated Short Range Communication
DBAP	Distance-Based Attacker Placement
GTSR	Global Tracking Success Rate
HTS	High Traffic Section
OBU	On-Board Unit
PMT	Pseudonym Management Technique
PRD	Periodic pseudonym scheme
RSU	Roadside Unit
SBAP	Speed-based attacker placement
SCMS	Security Credential Management System
SLOW	Silence at LOW speeds
TSI	Traffic/Stop Intersection
TSR	Tracking success rate
VANET	Vehicular Ad-hoc Network
VIN	Vehicle identification number
V2V	Vehicle-to-Vehicle Communication
V2I	Vehicle-to-Infrastructure Communication

References

1. Harnstein, H.; Laberteaux, L.P. A tutorial survey on vehicular ad hoc networks. *IEEE Commun. Mag.* **2008**, *46*, 164–171. [\[CrossRef\]](#)
2. IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Multi-Channel Operation. IEEE Std 1609.4-2016 (Revision of IEEE Std 1609.4-2006). Available online: https://standards.ieee.org/standard/1609_4-2016.html (accessed on 10 September 2020).
3. Kenney, J. Dedicated Short-Range Communications (DSRC) Standards in the United States. *Proc. IEEE* **2011**, *99*, 1162–1182. [\[CrossRef\]](#)
4. DSRC Committee. *Dedicated Short Range Communications (DSRC) Message Set Dictionary*; SAE Std. J2735; SAE Int.: Warrendale PA, USA, 2009.
5. Golle, P.A. On the anonymity of home/work location pairs. In Proceedings of the International Conference on the Pervasive Computing, Nara, Japan, 9–13 March 2009; Springer: Berlin/Heidelberg, Germany, 2009.
6. Duckham, M.; Kulik, L. *Location Privacy and Location-Aware Computing in Dynamic & Mobile GIS: Investigating Change in Space and Time*; Drummond, J., Ed.; CRC Press: Boca Raton, FL, USA, 2006; pp. 34–51.
7. Emara, K.; Woerndl, W.; Schlichter, J. *Beacon-Based Vehicle Tracking in Vehicular Ad-Hoc Networks*; Technical Report; Technische Universitat Munchen: Munchen, Germany, 2013.
8. Gerlach, M. Assessing and improving privacy in VANETs. In Proceedings of the 4th Workshop ESCAR, Berlin, Germany, 14–15 November 2006; pp. 1–9.
9. 1609.2-2016-IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages. Available online: <https://standards.ieee.org/standard/1609.2-2016.html> (accessed on 10 February 2020).
10. Buttyan, L.; Holczer, T.; Vajda, I. On the effectiveness of changing pseudonyms to provide location privacy in vanets. In *European Workshop on Security in Ad-Hoc and Sensor Networks*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 129–141.
11. Li, M.; Sampigethaya, K.; Huang, L.; Poovendran, R. Swing & swap: User-centric approaches towards maximizing location privacy. In Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, Alexandria, VA, USA, 30 October 2006; pp. 19–28.
12. Freudiger, J.; Raya, M.; Felegyhazi, P.P.; Papadimitratos, P.; Hubaux, J.P. Mix-zones for location privacy in vehicular networks. In Proceedings of the ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiNITS), Vancouver, BC, Canada, 14 August 2007; ACM: New York, NY, USA, 2007.
13. Brecht, B.; Theriault, D.; Weimerskirch, A.; Whyte, W.; Kumar, V.; Hehn, T.; Goudy, R. A Security Credential Management System for V2X Communications. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3850–3871. [\[CrossRef\]](#)
14. Buttyan, L.; Holczer, T.; Weimerskirch, A.; Whyte, W. SLOW: A Practical pseudonym changing scheme for location privacy in VANETs. In Proceedings of the 2009 IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, 28–30 October 2009; pp. 1–8.
15. Song, J.-H.; Wong, V.W.; Leung, V.C. Wireless location privacy protection in vehicular ad-hoc networks. *Mob. Netw. Appl.* **2010**, *15*, 160–171. [\[CrossRef\]](#)
16. Pan, Y.; Li, J. Cooperative pseudonym change scheme based on the number of neighbors in vanets. *J. Netw. Comput. Appl.* **2013**, *36*, 1599–1609. [\[CrossRef\]](#)
17. Emara, K.; Wolfgang, W.; Johann, S. CAPS: Context-aware privacy scheme for VANET safety applications. In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, New York, NY, USA, 22 June 2015.
18. Liao, J.; Li, J. Effectively changing pseudonyms for privacy protection in vanets. In Proceedings of the 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), Kaohsiung, Taiwan, 14–16 December 2009; pp. 648–652.
19. Wasef, A.; Shen, X. Rep: Location privacy for vanets using random encryption periods. *Mob. Netw. Appl.* **2010**, *15*, 172–185. [\[CrossRef\]](#)
20. Weerasinghe, H.; Fu, H.; Leng, S.; Zhu, Y. Enhancing unlinkability in vehicular ad hoc networks. In Proceedings of the 2011 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 10–12 July 2011; pp. 161–166.

21. Ullah, I.; Wahid, A.; Shah, M.A.; Waheed, A. VBPC: Velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET. In Proceedings of the 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, 19–21 April 2017; pp. 132–137.
22. Scheuer, F.; Fuchs, K.-P.; Federrath, H. A safety-preserving mix zone for vanets. In Proceedings of the International Conference on Trust, Privacy and Security in Digital Business, Toulouse, France, 29 August–2 September 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 37–48.
23. Eckhoff, D.; Sommer, C.; Gansen, T.; German, R.; Dressler, F. Strong and affordable location privacy in vanets: Identity diffusion using time-slots and swapping. In Proceedings of the 2010 IEEE Vehicular Networking Conference (VNC), Jersey City, NJ, USA, 13–15 December 2010; pp. 174–181.
24. Benarous, L.; Kadri, B.; Boudjit, S. Alloyed Pseudonym Change Strategy for Location Privacy in VANETs. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2020; pp. 1–6. [\[CrossRef\]](#)
25. Santos-Jaimes, L.M.; dos Santos Moreira, E. Pseudonym change strategy based on the reputation of neighboring vehicles in VANETs. *DYNA* **2019**, *86*, 157–166. [\[CrossRef\]](#)
26. Liu, Z.; Zhang, L.; Ni, W.; Collings, I. Uncoordinated Pseudonym Changes for Privacy Preserving in Distributed Networks. *IEEE Trans. Mob. Comput.* **2019**, *19*, 1465–1477. [\[CrossRef\]](#)
27. Boualouache, A.; Moussaoui, S. Tapcs: Traffic-aware pseudonym changing strategy for vanets. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 1008–1020. [\[CrossRef\]](#)
28. Singh, P.K.; Chourasiya, D.; Singh, A.; Nandi, S.K.; Nandi, S. CCAPS: Cooperative Context Aware Privacy Scheme for VANETs. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25 September 2019; pp. 1–5.
29. Zeng, M.; Xu, H. Mix-Context-Based Pseudonym Changing Privacy Preserving Authentication in VANETs. *Mob. Inf. Syst.* **2019**, *2019*, 3109238. [\[CrossRef\]](#)
30. Zhao, Z.; Ye, A.; Meng, L.; Zhang, Q. Pseudonym Changing for Vehicles in VANETs: A Game-Theoretic Analysis Based Approach. In Proceedings of the 2019 International Conference on Networking and Network Applications (NaNA), Daegu, Korea, 10–13 October 2019; pp. 70–74. [\[CrossRef\]](#)
31. Yang, M.; Feng, Y.; Fu, X.; Qian, Q. Location privacy preserving scheme based on dynamic pseudonym swap zone for Internet of Vehicles. *Int. J. Distrib. Sens. Netw.* **2019**. [\[CrossRef\]](#)
32. Li, W.; Song, H. ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2015**, *17*, 960–969. [\[CrossRef\]](#)
33. Wang, J.; Hari, S. Detecting Compromised Certificate Authority. U.S. Patent No. 9,686,081. 20 January 2017.
34. Emara, K. Poster: “Prext: Privacy extension for veins vanet simulator”. In Proceedings of the Vehicular Networking Conference (VNC), Columbus, OH, USA, 8–10 December 2016.
35. Saini, I.; Saad, S.; Jaekel, A. Attacker Placement for Detecting Vulnerabilities of Pseudonym Change Strategies in VANET. In Proceedings of the 1st International Workshop on Dependable Wireless Communications (DEWCOM), Chicago, IL, USA, 27–30 August 2018.
36. Saini, I.; Saad, S.; Jaekel, A. Speed Based Attacker Placement for Evaluating Location Privacy in VANET. In *Ad Hoc Networks ADHOCNETS 2018*; Springer: Cham, Switzerland, 2018.
37. Wiedersheim, B.; Ma, Z.; Kargl, F.; Papadimitratos, P. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In Proceedings of the 2010 Seventh International Conference on Wireless On-Demand Network Systems and Services (WONS), Kranjska Gora, Slovenia, 3–5 February 2010; pp. 176–183.
38. Kalman, R. A new approach to linear filtering and prediction problems. *Trans. ASME J. Basic Eng.* **1960**, *82*, 35–45. [\[CrossRef\]](#)
39. Fitzgerald, R.J. Development of practical pda logic for multitarget tracking by microprocessor. In Proceedings of the American Control Conference, Seattle, WA, USA, 18–20 June 1986; pp. 889–898.
40. Google Maps Platform—Traffic Layer. Available online: <https://developers.google.com/maps/documentation/javascript/examples/layer-traffic> (accessed on 8 May 2020).
41. Sommer, C.; German, R.; Dressler, F. Bidirectionally coupled network and road traffic simulation for improved IVC analysis. *IEEE Trans. Mob. Comput.* **2011**, *10*, 3–15. [\[CrossRef\]](#)

42. Varga, A.; Rudolf, H. An overview of the OMNeT++ simulation environment. In Proceedings of the 1st Inter-National Conference on Simulation Tools and Techniques for Communications, Networks and Systems and Workshops, Marseille, France, 3–7 March 2008; ICST(Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, Belgium, 2008.
43. Krajewicz, D.; Erdmann, J.; Behrisch, M.; Bieker, L. Recent development and applications of SUMO-Simulation of Urban MObility. *Int. J. Adv. Syst. Meas.* **2012**, *5*, 55031451.
44. OpenStreetMap. Available online: <https://www.openstreetmap.org/copyright> (accessed on 6 June 2019).



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).