Verification and Inference of Positions in Vehicular Networks through Anonymous Beaconing

# Verification and Inference of Positions in Vehicular Networks through Anonymous Beaconing

Francesco Malandrino, *Member, IEEE,* Carlo Borgiattino, *Student Member, IEEE* Claudio Casetti, *Member, IEEE,* Carla-Fabiana Chiasserini, *Senior Member, IEEE,* Marco Fiore, *Member, IEEE,* and Roberto Sadao, *Student Member, IEEE*

**Abstract**—A number of vehicular networking applications require continuous knowledge of the location of vehicles and tracking of the routes they follow, including, e.g., real-time traffic monitoring, e-tolling, and liability attribution in case of accidents. Locating and tracking vehicles has however strong implications in terms of security and user privacy. On the one hand, there should be a mean for an authority to verify the correctness of positioning information announced by a vehicle, so as to identify potentially misbehaving cars. On the other, public disclosure of identity and position of drivers should be avoided, so as not to jeopardize user privacy. In this paper, we address such issues by introducing A-VIP, a secure, privacy-preserving framework for continuous tracking of vehicles. A-VIP leverages anonymous position beacons from vehicles, and the cooperation of nearby cars collecting and reporting the beacons they hear. Such information allows a location authority to verify the positions announced by vehicles, or to infer the actual ones if needed, without resorting to computationally expensive asymmetric cryptography. We assess the effectiveness of A-VIP via realistic simulation and experimental testbeds.

**Index Terms**—Vehicular networks, position verification, privacy.

## 1 Introduction

Borrowing from a well-established communication pattern in wireless LANs, vehicular networks have adopted the term *beaconing* to indicate the periodic broadcasting of messages to neighboring vehicles or road-side units (RSUs). These messages, defined, e.g., in the SAE J2735 specifications, can be used for safety purposes as well as for cooperative awareness. The information they carry (e.g., vehicle ID, timestamps and location information) may be secured through the use of an on-board tamper-proof Hardware Security Module (HSM) as well as signatures, cryptography and certificates [1].

Secure beacons for vehicle position identification and tracking are needed in a number of scenarios where vehicle position accountability is a requirement in order to provide services to the community or to drivers. Secure reporting of vehicle location can substantiate drivers' claims in case of accidents. At the same time, secure location verification by authorities can provide accountability for those involved.

However, ensuring secure positioning must cope with three major problems, concerning (i) users' privacy, (ii) computational costs of security and (iii) the system trust on user correctness. As for the first aspect, when not strictly required, public disclosure of the vehicle identity to all receiving devices in the proximity of a beaconer is an issue. Vehicles can be tracked, jeopardizing drivers' privacy and requiring complex pseudonym management [2]. Thus, there is a need for separating secure position identification by authorities and the possibility of undesirable user tracking by peers in the vehicular network. As for the second aspect, standard security mechanisms based on, e.g., asymmetric cryptography, induce significant protocol overhead and computational complexity. In fact, their use is recommended to be largely dependent on the applications and circumstances, and avoided whenever possible [3]. Finally, basic solutions cannot guarantee the correctness of the location information provided by a user who owns the required cryptographic material, but has a malfunctioning GPS receiver or can tamper with GPS data before they are input to the HSM.

In this paper, we address the issues above by proposing A-VIP (Anonymous Verification and Inference of Positions), a framework that, unlike previous work:

*(i)* allows a trusted authority to securely collect and verify the positions claimed by vehicles without resorting to computationally expensive asymmetric cryptography – as is instead done in the IEEE 1609.2 standard [4];

*(ii)* in presence of unverified location claims, grants the authority the capability to infer the actual position of malfunctioning or misbehaving vehicles;

*(iii)* does so by safeguarding drivers' privacy with respect to other vehicles participating in the network, and without any requirement for uninterrupted radio coverage from road-side infrastructure.

*F. Malandrino, C. Borgiattino, C. Casetti and C.-F. Chiasserini are with Politecnico di Torino, Torino, Italy.*
*M. Fiore is with CNR–IEIIT, Torino, Italy and INRIA, Lyon, France.*
*R. Sadao is with Universidade de São Paulo, São Carlos, Brazil.*

To achieve such goals, A-VIP leverages *anonymous position beacons* from vehicles, which prevent overhearing nodes from identifying or tracking their source, but still allow authorized third parties – sharing secret information with the beaconing vehicles – to perform such operations. Then, an authenticated reciprocal beacon reporting scheme grants an authority the possibility to verify the locations claimed by vehicles and infer unverified positions by efficiently solving an optimization problem.

The rest of the paper is organized as follows. After reviewing related work in Sec. 2, we describe the system scenario and communication protocol in Sec. 3. Sec. 4 details the location verification and inference procedures, while Sec. 5 discusses the resilience of A-VIP to attacks by adversarial vehicles. The performance of A-VIP in both simulated and real-road environments is shown in Sec. 6. Finally, Sec. 7 concludes the paper.

## 2 Related Work

When considering the problem of location verification and inference, an extensive literature can be found in the domain of wireless sensor networks, including among others [5]–[8]. However, it is commonly acknowledged that solutions designed for static nodes do not fit the highly mobile vehicular scenarios we target.

Specific to the vehicular environment, many works have focused on pure ad-hoc vehicular network environments where no infrastructure or central authorities are considered. There, the aim is the verification of reciprocal position information so as to secure cooperative awareness and multihop routing. To that end, a number of different solutions have been proposed that leverage diverse metrics, including the distance among nodes and their relative mobility [9], [10], the Time-of-Flight (ToF) distance bounding [11] and ranging [12], the Received Signal Strength (RSS) within a two-hop neighborhood [13], or the presence of Non Line-of-sight (NLOS) conditions [14]. There have also been proposals to use dedicated hardware, such as multiple directional antennas [15], or original data structures, such as trusted routing tables [16].

With A-VIP, we take a different approach, considering the problem of vehicle position verification from the viewpoint of a trusted authority that collects car-generated location information through a roadside or cellular infrastructure. To the best of our knowledge, ours is the first attempt at designing a position verification system that considers such a perspective – which, although less visionary than the ad-hoc one, is more consistent with that expected to be the most viable architecture for secure vehicular communication systems [17]. Thus, our optimization problem formulation and the resulting centralized solution are hardly comparable with the techniques presented in the papers mentioned before.

We also remark that A-VIP does not only allow for position verification, but also addresses the problem of inferring the location of untrusted cars, and does so by granting user anonymity. Solutions have been proposed that specifically tackle the latter problems individually, such as [18], [19], but ours is the first work to present a comprehensive framework for secure, privacy-preserving localization.

Finally, our work is the first to experimentally evaluate the performance of a position verification and inference system through real-world testbeds.

## 3 Anonymous Positioning Procedure

We consider a WAVE-based vehicular network composed of vehicles communicating with each other and, occasionally, with RSUs. No assumption is made on the deployment of RSUs, so vehicles may travel along road segments where no RSU coverage is available. Vehicles may have also a 3G/LTE radio interface, through which they can access the cellular network that fully covers the road topology. Both RSUs and cellular base stations allow vehicles to contact a Location Authority (LA), which is in charge of collecting location claims, verifying them and inferring the actual positions of vehicles deemed to announce incorrect locations.

Vehicles are equipped with GPS, thus, unless otherwise specified, they know their own position and share a common time reference. Each vehicle owns cryptographic material, i.e., a certified identity and a long-term secret key, used to establish a secure channel with the LA at any time, through either an RSU or the cellular infrastructure. Solutions already exist for the distribution and management of long-term pairwise keys in vehicular environments (see, e.g., [4], [17]), and their discussion is out of the scope of this paper.

Vehicles that comply with the A-VIP mechanism are defined as *correct*, while the others may be: (i) *faulty*, that is, they follow the protocol but provide incorrect information due to, e.g., GPS malfunctioning, or (ii) *adversarial*, i.e., their aim is to announce a fake position and have it verified, so as to obtain some advantage, discredit nearby users, or disrupt the A-VIP operation. To that end, adversarial nodes can either deviate from the A-VIP communication protocol procedure, or comply with it but inject false information. In this work, we consider internal adversaries, more challenging than external ones, as they own the cryptographic material to participate in the protocol. We consider however that adversaries are unable to forge messages on behalf of other nodes whose keys they do not have. Adversaries may be further distinguished as independent or colluding: in this paper we focus on the former. However, in our analysis we also evaluate Sybil attacks, which can be viewed as a worst case of an attack carried out by colluding adversaries.

### 3.1 A-VIP goals

A-VIP aims at verifying the positions announced by correct vehicles while guaranteeing their privacy with respect to the other ones, and at detecting faulty or adversarial nodes while inferring their actual locations. Such goals are to be achieved with low computational complexity.

We stress that, barring the use of complex pseudonym management schemes [2], anonymity *cannot* be implemented simply by letting a vehicle issue beacons where its

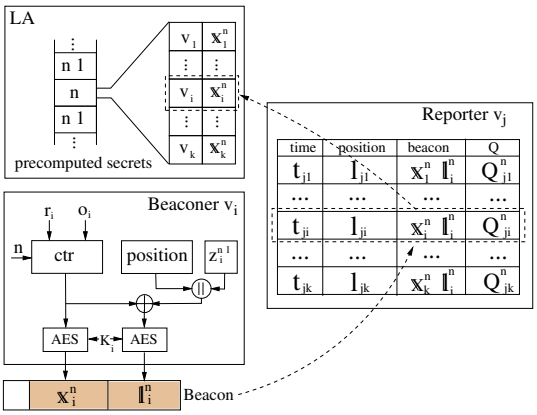



Fig. 1. A-VIP procedures by beaconer, reporter and LA.

identity is encrypted with the long-term shared key it shares with the LA. Indeed, some form of plaintext ID, attached to the encrypted beacon, would be needed for the LA to recognize the beacon originator and choose the appropriate key to decrypt the remainder of the message. Clearly, the presence of a plaintext ID would jeopardize the vehicle privacy, whose protection is one of our goals, allowing for overhearing and tracking by unauthorized receivers.

Additionally, we cannot just rely on encrypted cellular upload of the positioning information by vehicles. As a matter of fact, A-VIP is designed to be compatible with the cellular access infrastructure, but not to depend on it. More importantly, as discussed in Sec. 1, direct cellular upload does not allow for a verification of the location claimed by vehicles, which is instead part of the goals of A-VIP.

### 3.2 Communication procedures

The procedures in the A-VIP protocol are described below, while a schematic overview is shown in Fig. 1.

**Registration**. The registration procedure takes place every time a vehicle is started, and is repeated after a registration validity time has expired. It is performed over the secure channel between the vehicle and the LA, established with the long-term key via the RSU infrastructure, if available, or through 3G/LTE, otherwise.

Let us assume that a generic vehicle $v_i$ sends a registration request at time instant $t_{i,0}$. The LA records such an instant and returns to the vehicle a registration triplet ($K_i$, $r_i$, $o_i$) where $K_i$ is a short-term 128-bit AES symmetric key, and $r_i$, $o_i$ are random integers. The triplet is used to compute a time-dependent secret $\mathbb{x}_i(t)$, shared between the vehicle and the LA. As detailed later, when sent by $v_i$ to the LA, $\mathbb{x}_i(t)$ allows the LA to verify the freshness of a beacon transmission and the identity of its originator. In order to compute it, the two entities initialize a counter to $r_i$ and increment it by $o_i$ every $\tau_b$ seconds, e.g., at every beacon transmission. The updated counter is then encrypted with $K_i$ using AES in counter mode (AES-CTR) [20]. Thus, in general, if $t_{i,0} + n\tau_b \leq t < t_{i,0} + (n+1)\tau_b$, then $\mathbb{x}_i(t) = E_{K_i}\{r_i + no_i\} = \mathbb{x}_i^n$. Note that both $r_i$ and $o_i$ can be picked at random since the chances of collision among $\mathbb{x}^n$ values, related to different vehicles at the same time, are negligible.

The LA is then in a position to precompute all the upcoming values of $\mathbb{x}_i^n$ for a period that depends on the registration validity time. Clearly, the amount of memory needed by the LA to store precomputed values of $\mathbb{x}_i^n$ depends on the average number of vehicles in the area served by the LA and the time interval for which the $\mathbb{x}_i^n$ values are precomputed. As an example, in the scenario described in Sec. 6.1 and assuming a validity time equal to 1 hour, the required storage space at the LA for all vehicles amounts to an easily accommodated 52 Mbytes of memory.

**Anonymous beaconing**. When traveling, all correct vehicles broadcast a beacon every $\tau_b$, as foreseen by current standards. Beacon messages are broadcast by nature, and thus they are subject to undetected collisions over the wireless medium. While this may affect A-VIP operations, we stress that our approach can easily incorporate solutions to dynamically reduce channel contention such as [21]. For the purposes of this paper, we assume that all beacon transmissions occur at a power level common to all correct vehicles and at the basic data rate. Also, we assume the beacon to be split into two parts: an encrypted one, for the purposes set forth in this paper, and an unencrypted one, where plaintext content can be broadcast for such purposes as collision avoidance or cooperative awareness. We assume however that the beacon is anonymous, i.e., it does not include the vehicle identifier and it uses a fresh random MAC-layer address [17]. When not transmitting, the vehicle listens to the channel, overhearing beacons from other vehicles and collecting the information therein for later reporting to the LA.

The beacon content is assembled using the triplet assigned to a vehicle during the registration. Specifically, the $n$-th beacon issued by a vehicle $v_i$ carries two pieces of information, as shown in the "Beaconer" box of Fig. 1:

(a) the time-dependent secret $\mathbb{x}_i^n$, which can be computed by $v_i$ and by the LA, independently of each other;

(b) the encrypted current location announced by the vehicle $\mathbb{l}_i^n = E_{K_i}\{(\, l_i^n \,||\, z_i^{n-1}\,) \oplus (r_i + no_i)\}$, computed using the short-term pairwise key $K_i$ from the triplet. The plaintext location $l_i^n$ is concatenated with the one-bit flag $z_i^{n-1}$ used to notify the LA whether the beacon issued at step $n-1$ was affected by a replay attack (as explained in Sec. 5). Such a string is then XOR'ed with the plaintext counter value $(r_i + no_i)$, to ensure freshness of the beacon positioning content and thwart partial-replay attacks (as also detailed in Sec. 5).

**Reporting**. When a beacon issued by a vehicle $v_i$ is correctly received by a vehicle $v_j$, the latter is required to store the following entry in a *report table*, such as the one depicted in the "Reporter" box of Fig. 1:

- the time $t_{ji}$ at which the beacon is received;
- its own position $l_{ji}$ at the time the beacon was received;
- the secret $\mathbb{x}_i^n$ carried in the beacon;
- the encrypted position $\mathbb{l}_i^n$ of $v_i$ carried in the beacon;

- an optional field $Q_{ji}^n$, indicating the received signal quality (e.g., the received signal power computed by the radio interface driver).

Every $\tau_r$ seconds (report interval), $v_j$ generates a *report message* including the report table, populated with data collected from all newly overheard beacons. The report is transmitted to the LA, ensuring authentication and integrity through standard procedures. The transmission may occur via the RSU or via the cellular network if RSUs are scarce and real-time positioning is required. Additionally, multihop vehicle-to-vehicle communication can be exploited to reach nearby RSUs and, hence, speed up the report delivery.

We remark that vehicles normally act as both beaconers and reporters, and that the LA needs to receive only report messages, not the beacons broadcast by vehicles. Also, the communication procedures outlined above allow for a fully anonymous information exchange, preventing overhearing and thus ensuring user privacy.

## 4 Position Verification and Inference

When the LA receives reports from vehicles, it processes them so as to (i) determine the locations announced by cars in the system, (ii) verify such locations and (iii) infer the actual positions of vehicles deemed to have advertised an incorrect location.

Let the LA divide the road topology into discretized spatial *tiles*, whose set is denoted by $\mathcal{S}$. Also, let $\mathcal{V}$ be the set of vehicles that the LA has to verify. Upon receiving a report message from vehicle $v_j \in \mathcal{V}$, the LA processes one report table entry at a time, as follows:

- it extracts the time $t_{ji}$ at which $v_j$ received the beacon;
- for each $v_k \in \mathcal{V}$, it computes $n$ such that $t_{k,0} + n\tau_b \leq t_{ji} < t_{k,0} + (n+1)\tau_b$, i.e., $n = \lfloor (t_{ji} - t_{k,0})/\tau_b \rfloor$, and it looks up the precomputed secret value $\mathbb{x}_k^n$ that matches the $\mathbb{x}_i^n$ in the report table entry (LA box in Fig. 1).

When a match is found, the LA identifies $v_i$ as the vehicle that sent the beacon and retrieves the triplet associated to it [1]. Then, the LA performs the following actions:

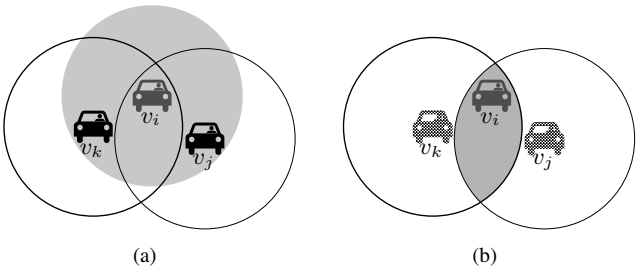
(1) it decrypts the $\mathbb{I}_i^n$ field entered by $v_i$ in the beacon reported by $v_j$, extracting the announced position $l_i^n$ and the flag $z_i^{n-1}$;

(2) if the $z_i^{n-1}$ flag is set, it discards the entry;

(3) otherwise, if $z_i^{n-1}$ is unset, it stores $n$, the position $l_i^n$ included in the beacon by $v_i$ and the position $l_j^n$ announced by $v_j$ in the report table entry. If present, the LA also stores the signal quality indicator, $Q_{ji}^n$, that $v_j$ measured on the beacon received from $v_i$.

The LA leverages the information extracted from the report table entry to identify the possible tiles corresponding to a vehicle position, thus verifying the location claim and possibly determining the actual vehicle location in case of mismatch. Clearly, the same beacon, characterized by a single $\mathbb{x}_i^n$, may be reported by multiple vehicles traveling in the proximity of $v_i$ when the latter broadcasted it. If so, the LA can obtain a better estimation of the beaconer position by combining the received reports. The steps required by this operation are detailed in the rest of this section, where, for sake of clarity, we drop the time notation and assume that all measures refer to the same beacon broadcast interval $n$.

1. If no match for $\mathbb{x}_i^n$ is found, the report entry is discarded. This may happen as a result of, e.g., replay attacks or node malfunctioning.




(a) (b)

Fig. 2. $Q$-unaware approach: $v_i$'s beacon is reported to the LA by $v_k$ and $v_j$. The shaded circle in (a) represents the transmission range of $v_i$, while the white circles denote the receiving range of $v_k$ and $v_j$. The shaded area in (b) represents the possible locations resulting from the combination of the two reports.

### 4.1 Cooperative position identification

Depending on whether the quality indicator $Q_{ji}$ is included in the report or not, the LA can adopt two different approaches to identify the tiles corresponding to the position of the beaconer $v_i$. The two techniques, named $Q$-unaware and $Q$-aware, operate as follows.

**The $Q$-unaware approach.** In this case, the LA does not have any information on the quality level with which the beacon signal was received at the reporter. Thus, for each pair of tiles $(s,t) \in \mathcal{S}^2$, it can assume a simple 0-1 propagation model to state whether a beacon sent from tile $s$ can be heard in $t$ or not, i.e., $h(s,t) : \mathcal{S}^2 \rightarrow \{0,1\}$. We remark that any methodology could be used to determine the vehicle radio range: from a simple unit disc model, displayed in Fig. 2, to a signal map drawn from real-world measurements [22].

Given that $v_j$ located in tile $t \in \mathcal{S}$ received the beacon from $v_i$, then the LA can identify a set of tiles, $\mathcal{S}_i^{(j)} \subseteq \mathcal{S}$, where the beaconer could have been. Due to the simple propagation model, all tiles in $\mathcal{S}_i^{(j)}$ correspond to the right location with equal probability. Thus, the probability that the beaconer was in tile $s$ when $v_j$ heard its beacon is given by:

$$p_{i,s}^{(j)} = \begin{cases} \frac{1}{|\mathcal{S}_i^{(j)}|} & \text{if } s \in \mathcal{S}_i^{(j)} \\ 0 & \text{otherwise}\,. \end{cases} \tag{1}$$

Note that, if multiple reports from correct nodes are available, the corresponding sets of tiles may intersect, as depicted in Fig. 2(b). In this case, the LA can obtain a better estimate of the true position of $v_i$. Considering the intersection translates into computing the following probability:

$$P_{i,s}^{(\mathcal{R}_i)} = \frac{\prod_{j:v_j \in \mathcal{R}_i} p_{i,s}^{(j)}}{\sum_{u \in \mathcal{S}} \prod_{j:v_j \in \mathcal{R}_i} p_{i,u}^{(j)}} \quad \forall s \in \mathcal{S}\,, \tag{2}$$

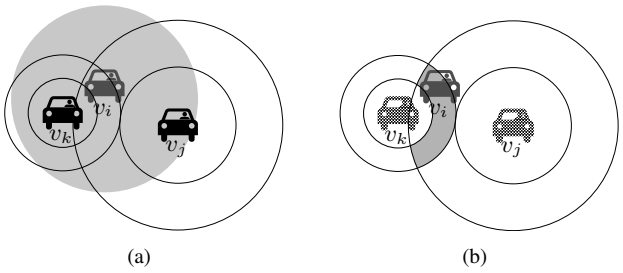



Fig. 3. Q-aware approach: the beacon from $v_i$ is reported by $v_k$ and $v_j$. The shaded area in (a) represents the transmission range of $v_i$. The annuluses denote the set of locations from which a beacon could be received by, respectively, $v_k$ and $v_j$ with the quality level indicated in their report. In (b), the intersection of the annuluses represents the possible positions of $v_i$.

where $\mathcal{R}_i$ is the set of vehicles that reported $v_i$'s beacon. We stress that $p_{i,s}^{(j)}$ represents the probability that $v_i$ was in $s$ while sending the beacon, computed taking only one report into account. $P_{i,s}^{(\mathcal{R}_i)}$ represents the same probability, yet computed by combining the information received from multiple correct reporters.

**The $Q$-aware approach.** When a report includes the $Q_{ji}$ value related to a beacon reception, such information can be exploited to refine the position estimate of beaconer $v_i$. To do so, the LA needs an accurate model of the propagation conditions in the area where the broadcast transmission took place, including received signal quality information. Again, deterministic (e.g., ray-tracing), stochastic, or measurement-based models can be used: the $Q$-aware procedure does not change and is performed as follows.

Let the propagation model be a function $h(s,t,Q_{ji}) : \mathcal{S}^2 \times \mathbb{R} \rightarrow [0,1]$ that, for any pair of tiles $(s,t)$ and any signal quality value $Q_{ji}$, provides the probability $\mathbb{P}(R_t^{(j)}|B_s^{(i)},Q_{ji})$ that a beacon sent by $v_i$ from tile $s$ can be received by $v_j \in \mathcal{R}_i$ in tile $t$, with the quality level $Q_{ji}$ reported by $v_j$.

By applying Bayes' theorem, the LA can use such values to compute the probability $\mathbb{P}(B_s^{(i)}|R_t^{(j)},Q_{ji})$ that the beaconer was in title $s$, given that the beacon was heard by $v_j$ in tile $t$, with a quality level $Q_{ji}$. Specifically,

$$p_{i,s}^{(j)} = \mathbb{P}(B_s^{(i)}|R_t^{(j)},Q_{ji}) = = \frac{\mathbb{P}(R_t^{(j)}|B_s^{(i)},Q_{ji}) \cdot \mathbb{P}(B_s^{(i)})}{\sum_{u \in \mathcal{S}} \mathbb{P}(R_t^{(j)}|B_u^{(i)},Q_{ji}) \cdot \mathbb{P}(B_u^{(i)})} \quad (3)$$

where $\mathbb{P}(B_x^{(i)})$, $x = s,u$, is the probability that the broadcasting vehicle $v_i$ is in tile $x$ at the time of transmission. This value may depend on the vehicle density and on the size of the considered area. We assume however a generic scenario where no such knowledge is available, and the probability is equally spread among all tiles, i.e., $\mathbb{P}(B_s^{(i)}) = 1/|\mathcal{S}|$ for any $v_i$ and any tile in $s \in \mathcal{S}$.

Upon receiving multiple reports, the LA can again resort to (2) to combine the $Q$-aware probabilities computed as in (3). Then, it can determine the tiles the beaconer could have been at the moment of the broadcast, with the associated probabilities $P_{i,s}^{(\mathcal{R}_i)}$. Note that, unlike the $Q$-unaware case, such probabilities are now $Q$-dependent and provide better location estimates, assuming that the underlying signal quality model is accurate enough.

A simple example of the $Q$-aware approach is portrayed in Fig. 3, where two reporters, $v_k$ and $v_j$, include different quality levels for a beacon received from $v_i$. For simplicity, in the figure we considered that the area corresponding to the value of $Q$, indicated by a reporter, maps onto an annulus comprised in its reception range. Then, the set of possible locations of the beaconer is given by the intersection of the two annuluses, i.e., the shaded area in Fig. 3(b).

### 4.2 Assessing the trustworthiness of vehicles

The technique used in the previous subsections to combine multiple reports assumes that all reports come from correct nodes. Unfortunately, as we discussed in Sec. 1, faulty or adversarial users may report fake position information and invalidate any attempt by the LA to estimate their own and other vehicles' positions. Thus, it is therefore essential to determine the *trustworthiness* of vehicles in order to tell apart faulty or adversarial nodes. A-VIP performs this task by leveraging the information contained in reports sent by vehicles. Hence, the trust attribution process described below is only performed, within each time step, for the subset $\overline{\mathcal{V}} \subseteq \mathcal{V}$ of vehicles that satisfy two conditions: (i) having transmitted a beacon and (ii) having had such beacon reported by others.

The trustworthiness probability of vehicle $v_i$ at a generic time step, which we will refer to as $\gamma_i \in [0,1]$, is determined by the LA through a three-phase process:

(1) the *location probability* $\Phi_{i,s}^{(\mathcal{R}_i)}$ that $v_i$ is at any tile $s \in \mathcal{S}$ upon beacon transmission is computed by taking into account the (unknown) trustworthiness of vehicles in $\mathcal{R}_i$, i.e., those that reported the beacon sent by $v_i$;

(2) the location and trustworthiness probabilities of all vehicles in $\overline{\mathcal{V}}$ are combined into a global *consistency function*, $\chi$, corresponding to the average number of vehicles that are correctly estimated to be in their declared location;

(3) the trustworthiness probability $\gamma_i$ of each vehicle in $\overline{\mathcal{V}}$ is computed so that the consistency function $\chi$ is maximized.

Phase one above is achieved by letting the LA combine the information it received in the reports in a similar fashion as that of (2). This time, however, the unknowns represented by the trustworthiness of the vehicles participating in the process are integrated in the expression. Specifically, for each $s \in \mathcal{S}$, the LA evaluates the location probability $\Phi_{i,s}^{(\mathcal{R}_i)}$ that $v_i$ was in tile $s$ when sending the beacon, as:

$$\Phi_{i,s}^{(\mathcal{R}_i)} = \sum_{\mathcal{Z} \in \wp(\mathcal{R}_i)} \left( P_{i,s}^{(\mathcal{Z})} \prod_{j:v_j \in \mathcal{Z}} \gamma_j \prod_{k:v_k \in \mathcal{R}_i \setminus \mathcal{Z}} (1-\gamma_k) \right). \quad (4)$$

In (4), $\wp(\mathcal{R}_i)$ is the power set of $\mathcal{R}_i$, i.e., all possible subsets (proper and not) of reporters in $\mathcal{R}_i$. The terms $P_{i,s}^{(\mathcal{Z})}$ are calculated as in (2), using the probabilities $p_{i,s}^{(j)}$. Recall

that the latter probabilities are computed using either (3) or (1), depending on whether the information on the $Q$-value is available or not. Also, we define $P_{i,s}^{(\emptyset)} = \mathbb{P}(B_s^{(i)})$. In words, the expression in (4) states that, if only the reporters in the subset $\mathcal{Z}$ are trustworthy, which happens with probability $\prod_{j:v_j\in\mathcal{Z}} \gamma_j \cdot \prod_{k:v_k\in\mathcal{R}_i\setminus\mathcal{Z}}(1-\gamma_k)$, then the probability that the beaconer $v_i$ was in $s$ is obtained by considering the reports sent by such vehicles ($v_j \in \mathcal{Z}$) and neglecting the others ($v_k \in \mathcal{R}_i\setminus\mathcal{Z}$). Consistently, the term $P_{i,s}^{(\emptyset)}$ corresponds to the case where no trustworthy vehicle exists, hence the probability that $v_i$ was in $s$ is $\mathbb{P}(B_s^{(i)})$, which does not depend on any report. Finally, note that, if $\gamma_j = 1\ \forall j : v_j \in \mathcal{R}_i$, the expression in (4) reduces to $P_{i,s}^{(\mathcal{R}_i)}$, i.e., to the probability associated to the intersection of all the reported beacon receptions, as illustrated in Sec. 4.1.

In the second phase, the LA defines the global *consistency function*, $\chi$, as the (expected) number of correctly estimated positions for vehicles in $\overline{\mathcal{V}}$:

$$\chi = \sum_{i:v_i\in\overline{\mathcal{V}}} \left( \gamma_i \Phi_{i,l_i}^{(\mathcal{R}_i)} + (1-\gamma_i) \sum_{s\in\mathcal{S}} \Phi_{i,s}^{(\mathcal{R}_i)} \right). \quad (5)$$

For each vehicle $v_i$, the first term of the sum in (5) corresponds to the case where $v_i$ is correct (which happens with probability $\gamma_i$), and it represents the probability that $v_i$ was in the tile including the position $l_i$ that it announced in its beacon. The second term, instead, corresponds to the case where $v_i$ cannot be trusted (which happens with probability $1-\gamma_i$) and it accounts for the probability that $v_i$ could have been in any of the possible tiles, $s \in \mathcal{S}$. Note that the expression in (5) has the following interesting property: when all vehicles are trustworthy, i.e., $\gamma_i = 1\ \forall i$, it reduces to $\chi = \sum_{i:v_i\in\overline{\mathcal{V}}} P_{i,l_i}^{(\mathcal{R}_i)} \leq |\overline{\mathcal{V}}|$. In this case, $\chi$ is a measure of the accuracy of the estimation based on the cooperative position identification described in Sec. 4.1, which correctly increases as $\chi$ approaches $|\overline{\mathcal{V}}|$.

In phase three, the LA determines the trustworthiness $\gamma_i$ of each vehicle in $\overline{\mathcal{V}}$ by solving following problem:

$$\begin{aligned} \max \quad & \textstyle\sum_{i:v_i\in\overline{\mathcal{V}}} \left( \gamma_i \Phi_{i,l_i}^{(\mathcal{R}_i)} + \delta_i \sum_{s\in\mathcal{S}} \Phi_{i,s}^{(\mathcal{R}_i)} \right) \\ s.t. \quad & \Phi_{i,s}^{(\mathcal{R}_i)} = \textstyle\sum_{\mathcal{Z}\in\wp(\mathcal{R}_i)} \left( P_{i,s}^{(\mathcal{Z})} \prod_{j:v_j\in\mathcal{Z}} \gamma_j \prod_{k:v_k\in\mathcal{R}_i\setminus\mathcal{Z}} \delta_i \right) \\ & 0 \leq \gamma_i \leq 1 \quad 0 \leq \delta_i \leq 1 \quad \gamma_i + \delta_i = 1\,. \end{aligned}$$

In the problem above, the objective imposes to maximize the consistency $\chi$. The first constraint enforces the definition of $\Phi$, and is equivalent to (4). The second constraint ensures that $\gamma$ values are between 0 and 1. The last two constraints introduce a set of auxiliary variables $\delta_i = 1-\gamma_i$. By introducing these variables in the problem, we make the objective *posynomial*[2]. Posynomial problems can be reduced to a convex form and thus maximized in polynomial time [23].

2. A posynomial is a function of the form $f(x_1, x_2, \ldots, x_n) = \sum_{k=1}^{K} c_k x_1^{a_{1k}} \cdots x_n^{a_{nk}}$ where all $x_i$ and coefficients $c_k$ are positive real numbers, and the exponents $a_{ik}$ are real.

**Algorithm 1** Identifying the set of trustworthy vehicles.

**Require:** $\gamma_i,\ \forall v_i \in \overline{\mathcal{V}}$
1: $\mathcal{T} \leftarrow \emptyset$
2: $\mathcal{T}' \leftarrow \emptyset$
3: **repeat**
4: $\quad \mathcal{T} \leftarrow \mathcal{T}'$
5: $\quad v_i \leftarrow \arg\max_{h:v_h\in\overline{\mathcal{V}}\setminus\mathcal{T}} \gamma_h$
6: $\quad \mathcal{T}' \leftarrow \mathcal{T} \cup \{v_i\}$
7: **until** $\left(\exists v_k\colon v_i \in \mathcal{R}_k \wedge \max_{\mathcal{S}} P_{k,s}^{(\mathcal{T}_k')} = 0\right) \vee \mathcal{T}' = \overline{\mathcal{V}}$
8: **return** $\mathcal{T}$

### 4.3 Detecting fake identities

The above mechanism is based on the consistency among the reported positions of all vehicles. However, it may not be sufficient against Sybil attackers, which control multiple identities and use them to consistently report false positions. To this end, we put in place a specific mechanism to uncover fake identities, named *buddy detection*.

The key idea is fairly simple: if two (or more) vehicles *consistently* appear to be colocated, there is something suspicious. More formally, we say that two vehicles $v_i$ and $v_j$ consistently appear to be together if the sets $\mathcal{R}_i^k$ and $\mathcal{R}_j^k$ overlap for more than a fraction $f$, i.e., if

$$\sum_k |\mathcal{R}_i^k \cap \mathcal{R}_j^k| \geq f \cdot \min\left( \sum_k |\mathcal{R}_i^k|, \sum_k |\mathcal{R}_j^k| \right). \quad (6)$$

If the above condition is verified, we set $\gamma_i = \gamma_j = 0$, i.e., the LA declares both $v_i$ and $v_j$ as non-trustworthy. Note that the minimum in (6) implies that an attacker alternating several fake identities will still be detected.

The parameter $f$ should be set taking into account two factors. First, some beacons and reports may be lost, and the overlap between the sets may be not complete. Second, an attacker controlling more than $f \cdot |\mathcal{R}_i|$ fake identities will not be detected. In Sec. 6.3, we show the effectiveness of the buddy detection mechanism in terms of false positives/negatives, already for low values of $f$.

### 4.4 Deriving the vehicle positions

As a result of the above procedure, the LA obtains the $\gamma_i$ values for all vehicles in $\overline{\mathcal{V}}$, i.e., those that, during the time step under consideration, have broadcast a beacon that was then reported to the LA. Then, the LA can run Alg. 1 with the goal to determine the set $\mathcal{T} \subseteq \overline{\mathcal{V}}$ of vehicles deemed to be trustworthy.

At the outset, the LA initializes the set of trustworthy vehicles, $\mathcal{T}$, to the empty set (line 1). Then, at each step, it selects the vehicle $v_i$ in $\overline{\mathcal{V}}$, but not in $\mathcal{T}$ yet, for which the probability to be trustworthy is the highest. It adds the vehicle to the set $\mathcal{T}'$, which is thus given by $\mathcal{T} \cup \{v_i\}$ (lines 5–6). If the information provided by $v_i$ is consistent with the one provided by vehicles already in $\mathcal{T}$, then $v_i$ is deemed trustworthy as well and included in $\mathcal{T}$.

More precisely, let us denote by $\mathcal{T}'_k$ the set of vehicles that have reported the beacon sent by $v_k$ and are in set $\mathcal{T}'$. Then, for each vehicle $v_k$, for which $v_i$ has reported a consistent information with respect to all other trustworthy reporters, there will be at least one tile $s$ with non-zero probability, $P_{k,s}^{(\mathcal{T}'_k)}$, associated to it (line 7). That is, the intersection among the location sets corresponding to the reports sent by the trustworthy vehicles and by $v_i$ will not be empty. If this is the case, $v_i$ is added to $\mathcal{T}$ (line 4). Otherwise, $v_i$, and all the reporters with a value of trustworthiness probability lower than $\gamma_i$, are tagged as non-trustworthy, and the procedure ends. Thus, the last computed set $\mathcal{T}$ includes all vehicles in $\overline{\mathcal{V}}$ that are deemed to be trustworthy by the LA.

After running Alg. 1, for each vehicle $v_i$ in $\overline{\mathcal{V}}$, the LA determines the position set $\mathcal{L}_i \subseteq \mathcal{S}$ corresponding to the locations where the vehicle is deemed to be. In particular, if $v_i \in \mathcal{T}$, the LA considers the position $\mathcal{L}_i = \{l_i\}$, where $l_i$ is the location declared by $v_i$ in its beacon. Otherwise, the LA associates to $v_i$ the set of possible locations $\mathcal{L}_i = \{s | P_{i,s}^{(\mathcal{T}_i)} > 0\}$. Note that, if $v_i \notin \mathcal{T}$ and no trustworthy vehicle has reported the beacon from $v_i$, i.e., $\mathcal{T}_i = \emptyset$, we have $P_{i,s}^{(\emptyset)} = 0 \ \forall s \in \mathcal{S}$, hence $\mathcal{L}_i = \emptyset$ and no position estimation is available at this time instant for $v_i$.

As a last step, the LA checks for all vehicles in $\overline{\mathcal{V}}$, for which $\mathcal{L}_i \neq \emptyset$, if their location was missing at some of the previous time instants. Let us consider the case where the LA finds missing position information for $v_i$ at all time instants $k \in (n, n+T)$, while $\mathcal{L}_i^n$ and $\mathcal{L}_i^{n+T}$ are not empty. Then, the LA can estimate $\mathcal{L}_i^k$ as follows. For each pair of tiles $s \in \mathcal{L}_i^n$ and $u \in \mathcal{L}_i^{n+T}$, the LA exploits the empirical probability density function of the traveling time from $s$ to $u$ and verifies whether the probability that $v_i$ was in the generic tile $t \in \mathcal{S}$ at time $k$ is greater than 0. If so, $t$ is added to the set $\mathcal{L}_i^k$. By doing so, the LA obtains a set of possible positions for $v_i$ at $k$, along with their probabilities.

## 5 Attacks against A-VIP

Next, we discuss some possible attacks targeted at disrupting the position verification process described above. Our focus is on attacks orchestrated by single or multiple, albeit independent, adversaries. Colluding adversaries would indeed have the additional burden of continuous platooning to be successful, thus we consider these attacks as unpractical.

**Transmit-power attack**. The A-VIP position identification technique described in Sec. 4.1 relies on the fact that all correct vehicles transmit their beacons at the same power level. An attacker may maliciously increase or decrease its transmit power, thus affecting the $Q$-unaware and $Q$-aware approaches to the position verification and pretending to be closer or farther from the reporters than it actually is. However, while fooling a part of its neighbors, the attacker cannot help but appear inconsistent to the rest, since its announced position does not match the expected physical behavior of the transmission. Thus, A-VIP successfully detects transmit-power attacks, as shown in Sec. 6.3.

**False location attack**. It aims at pretending to be at a location different from the actual one, and at the same time at disrupting the operation of the beacon-reporting process. Specifically, the attack consists in a vehicle transmitting a beacon that includes the right time-dependent secret but a false position information. The announced position will not be coherent with the locations advertised by vehicles receiving the beacon in their reports, which may generate problems in the verification process. However, our results in Sec. 6.3 demonstrate that the A-VIP verification mechanism described in Sec. 4.2 is robust to this kind of attack.

**Replay attack**. Adversarial users replay beacons from correct vehicles. Although the attacker can retransmit a copy of the beacon, it cannot tamper with its content, as both the secret $\mathbb{x}_i^n$ and the beaconer position information are encrypted. We remark that encrypting the location $l_i^n$ together with the current counter value, as described in Sec. 3.2, univocally ties $l_i^n$ to $\mathbb{x}_i^n$. This prevents *partial replay* attacks, where the adversary only replays $\mathbb{x}_i^n$ and modifies the encrypted field $\mathbb{I}_i^n$ that contains the position information .

Still, by performing a full replay at locations other than those of the original broadcast, the attacker could induce the LA to tag correct nodes as faulty. In such cases, the timing of the replay is of the essence:

- in case of a replay attack occurring more than $\tau_b$ seconds after the legitimate beacon was broadcast, the LA will no longer be able to match the secret in the beacon with any precomputed secret during that time frame, and the report table entry will be ignored;
- in case of a replay attack occurring less than $\tau_b$ seconds after the legitimate beacon was broadcast, the replayed message will be reported multiple times by one or more witnesses. The LA will easily detect the presence of a duplicate, delayed entry in reports and reject it.

In the latter case, the trustworthiness of the original beacon sender would be tarnished. However, this sender can detect the replay of its own beacon and report the misdeed by setting the $z_i^{n-1}$ bit in its following beacon, as introduced in Sec. 3.2. Recall that $z_i^{n-1}$ can only be set by the original beacon sender, since it is encrypted along with the vehicle position within $\mathbb{I}_i^n$ and its freshness is ensured by the counter value. The LA will thus know that the beacon is invalid without affecting the vehicle credibility. The only result an attacker can achieve is thus to occasionally invalidate beacons from random vehicles. Jamming could yield the same effect with lower system complexity.

**Wormhole attack**. The replay attack can be combined with a wormhole attack, so that a full replay occurs less than $\tau_b$ seconds after the legitimate beacon was broadcast and in a different region (to avoid detection by the original sender). As a result, the replayed beacon will also be reported by witnesses other than those within the sender's communication range. In this case, the LA can detect the inconsistency by noting that the same beacon is heard by multiple witnesses farther apart than the nominal transmission range. The LA will thus be able to disregard both the original and replayed beacon entries without affecting the trustworthiness of the

original sender. Additionally, the information collected at the LA allows for locating the wormhole ends, which have to be placed within the communication range of the reporters receiving the duplicate beacon. Since A-VIP implicitly counteracts wormhole attacks, we do not experimentally assess its robustness to them.

**Phantom attack**. An adversarial vehicle can run a phantom attack by never broadcasting beacons, nor reporting to the LA: such a vehicle would thus be completely transparent to the system. Its advantages are dubious. If, on the one hand, the attack could be used by a vehicle who is trying to escape liability after causing a car wreck, on the other, a phantom attacker falsely accused of being involved in an accident would be unable to prove it was elsewhere.

Additionally, phantom attacks could pose a threat to commercial applications such as e-toll enforcement. In such cases, the onboard devices are required to be tamper-resistant HSMs integrating the antenna apparatus, so that no vehicle can successfully disappear from the network. For these reasons, countering this attack is out of the scope of A-VIP.

**Teleport attack**. An adversarial user could impair local transmissions of its own beacons and have a colluder broadcast those same beacons at a location other than that where it actually is. We refer to this as teleport attack, enabling the adversary to, e.g., deny liability in any accident in which she is involved by having her beacons broadcasted at a distant, safe location. The same discussion as for the phantom attack applies here as well, and an integrated-antenna HSM is required to prevent teleport attacks when the goal is determining liability. Thus, we do not assess the robustness of A-VIP to such attack.

**Sybil attack**. In a vehicular network, a Sybil attack is run by a single car that owns multiple identities and can thus impersonate several vehicles [24]. In the context of localization, a Sybil attacker can autonomously corroborate the fake position it advertises. More specifically, an adversarial user could avoid broadcasting beacons (i.e., perform a phantom attack), yet have multiple impersonated vehicles reciprocally (though falsely) report each other's beacons. Such attackers could thus claim any possible position.

We stress that Sybil attacks are difficult by nature. In a system of communicating vehicles, identities cannot be fabricated but they must have been legitimately obtained, hence successively stolen by the adversary. Such a hurdle makes the Sybil attack often infeasible, or only feasible for a short time before the identity theft is discovered.

Nonetheless, A-VIP is designed to cope this attack. The *buddy detection* procedure described in Sec. 4.3 aims precisely at discovering fake identities. We prove its effectiveness in Sec. 6.3.

## 6 Evaluation

Our evaluation of A-VIP is carried out in a simulated, yet realistic, vehicular scenario, as well as in real-world live testbeds. They are presented in Sec 6.1, along with the metric adopted to assess the quality of the A-VIP results, and in the Supplemental Material. Our simulative and experimental study has two main goals. Firstly, in Sec. 6.2 we aim at acquiring a better understanding of the accuracy of the position estimation provided by our framework. Secondly, in Sec. 6.3, we focus on testing the A-VIP resilience to a range of different attacks.

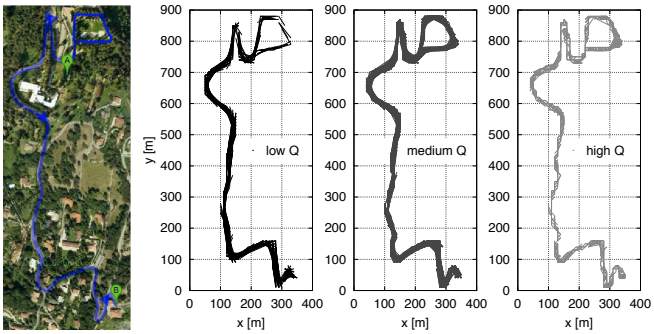



Fig. 4. Testbed: actual route (left) and RF signal maps.

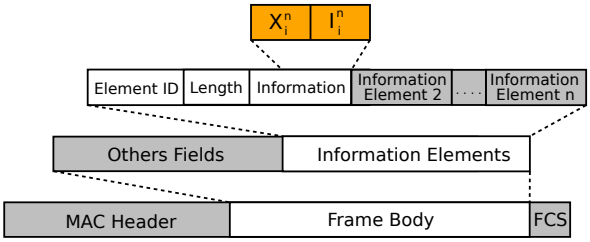



Fig. 5. Testbed: A-VIP information ($\mathbb{x}_i^n$ and $\mathbb{I}_i^n$, in yellow) integration in the legacy IEEE 802.11 beacon.

### 6.1 Scenarios and metrics

**Simulation scenario**. Simulations are run on a map representing a $1\times1.5$ km$^2$ section of the urban area of Ingolstadt, Germany. The scenario models a total of 2792 vehicles over a period of about 1 hour, with a mean trip time of 5 minutes and 24 seconds and a mean road traffic density of 300 vehicles per km$^2$ [19]. The vehicular mobility is generated using the well-known Simulator of Urban MObility (SUMO), capable of reproducing real-world microscopic and macroscopic road traffic. The RF signal propagation is modeled through the 802.11p/DSRC radio shadowing technique proposed in [22]. The model accounts for buildings, and has been validated via real-world measurements in urban environments. As a result of the coupling of the vehicular mobility and signal propagation, we record vehicles to have an average of 69.83 neighbors, i.e., potential reporters per beacon in A-VIP. The availability of RF signal propagation information in the evaluation scenario lets us leverage the Q-aware technique presented in Sec. 4.1 to compute the probabilities $p_{i,s}^{(j)}$. We also model the 802.11p channel access and collisions that may take place among simultaneous transmissions.

While assessing the impact of malicious behavior, we consider a challenging scenario where 10% of the vehicles are randomly selected as adversaries, unless otherwise specified.

**Experimental testbed**. We implemented the A-VIP protocol on commercial off-the-shelf hardware, in order to assess its position estimation capabilities and robustness to attacks in live testbeds. One of the testbeds is deployed in a urban area in the center of Turin, Italy, and is described, along with performance results, in the Supplemental Material. The testbed we present here covers instead a 2-km road loop nearby Turin, Italy, and is composed of portions of a public road and of a private road in a suburban woodland area. The testbed comprises 5 vehicles, which follow the route portrayed in the left image of Fig. 4. A single RSU is deployed in the testbed, providing intermittent Internet access to up to five vehicles circulating at a time in the road loop within each other's range for most of the time.

From a technical viewpoint, the RSU and the vehicles are equipped with an Alix PC Engines motherboard, with an AMD Geode 500 MHz processor and one Ubiquiti Networks XtremeRange 5 radio IEEE 802.11a card. Vehicles carry one 5-dBi omnidirectional antenna on their rooftops, and are configured to transmit at an output power of 18 dBm. Finally, GPS receivers provide vehicle localization data.

A-VIP is implemented as a user-level application capable of transmitting and receiving beacons in ad hoc mode between vehicles, and sending reports to the RSU. Beacons are generated and broadcast every $\tau_b$ seconds, which is a configurable system parameter. The beaconing application exploits native IEEE 802.11 beacons, by including the information required for A-VIP operation, i.e., the secret $\mathbb{x}_i^n$ and the encrypted location information $\mathbb{l}_i^n$ of the emitting vehicle $v_i$. Such data is 32-byte long and is injected in the Vendor Specific Information Element (Vendor IE) field of the 802.11 beacon, as depicted in Fig. 5, without any need to edit the wireless card drivers. Upon reception of a new beacon from $v_i$, a vehicle $v_j$ retrieves and stores the A-VIP data in its report table, along with a 4-byte reception time $t_{ji}$, a 8-byte current position $l_{ji}$ and a 1-byte received signal quality indicator $Q_{ji}^n$.

In our live testbed, the propagation model used for the $Q$-aware computation of the probabilities $p_{i,s}^{(j)}$ is derived from experimental measurements. The corresponding propagation map is depicted in the three right plots of Fig. 4, where, for clarity of presentation, the values of received signal power have been discretized into high (-40 to -60 dBm), medium (-60 to -80 dBm) and low (-80 to -95 dBm) signal quality bins. Consistently with intuition, we remark that shorter distances correspond to better signal quality.

In the case of attacks, we use 5 vehicles and randomly select 2 of them as adversaries.

**Location error**. In order to express the quality of the LA estimates, we introduce a metric called *location error*. Formally, for the $n$-th beacon issued by a vehicle $v_i$ whose actual position at the broadcast time is $\ell_i^n$, the location error is defined as follows:

$$e_i^n = \sum_{s \in \mathcal{L}_i^n} P_{i,s}^{(\mathcal{T}_i)} d(\ell_i^n, s)\,. \tag{7}$$

Note that, in case of a vehicle $v_i$ deemed trustworthy (i.e., $v_i \in \mathcal{T}$), $\mathcal{L}_i^n = \{l_i^n\}$, hence the location error represents the distance between its actual ($\ell_i^n$) and declared ($l_i^n$) positions. Thus, in this case $e_i^n$ = 0 if the vehicle is actually correct and its GPS is precise.

Instead, if $v_i$ is not deemed trustworthy, the location error is the average of the distances between its actual location and the centers of the tiles representing its possible locations. The average is weighted by the probability that $v_i$ is in each of such tiles $s \in \mathcal{L}_i^n$, according to trustworthy vehicles that received the $n$-th beacon from $v_i$ (i.e., $P_{i,s}^{(\mathcal{T}_i)}$). In this case, $e_i^n$ is the error that the LA incurs when trying to recover the actual position of an untrusted vehicle from the reports of trustworthy cars.

We stress that the second situation occurs also in the case of a vehicle $v_i$ announcing its position with a frequency lower than that used by the LA to verify locations. Indeed, this forces the LA to estimate the location of $v_i$, as described in Sec. 4.4. In the following, we set the reporting periodicity $\tau_r$ equal to the beaconing interval $\tau_b$, and consider that the LA verifies the position of all vehicles at every second, thus computing the location errors with a 1-Hz frequency.

### 6.2 A-VIP position estimation quality

We first assess the quality of the position estimation described in Sec. 4.1, both via simulation and our suburban live testbed, in absence of faulty or adversarial users. In this case, the uncertainty comes from the RF signal propagation, which is time-varying and may induce errors in the estimation process, possibly up to the point where some vehicles are tagged as untrustworthy. Additionally, beacons and reports may be lost due to channel errors, contributing to impair the verification by the LA.

**Simulation results**. Fig. 6 shows how the location error, averaged over all vehicles, is affected by different system parameters in the simulation scenario.

In Fig. 6(a), we assume that all vehicles periodically report to the LA according to the procedure described in Sec. 3.2, and we evaluate the impact of the per-vehicle beacon transmission periodicity $\tau_b$. Colors denote different spatial granularities (i.e., tile side lengths), ranging from 10 to 50 m. In these tests, A-VIP correctly tags all vehicles in the simulation as trustworthy, thus the framework does not generate any false positive. According to the location error definition in (7), the positions considered by the LA are those *declared* by the vehicles in their reports (solid lines in the plot). However, for the sake of completeness, we also report the error measured on positions *estimated* from other cars' reports through the $Q$-aware approach presented in Sec. 4.1 (dashed lines). This allows us to comment on the quality of the cooperative position identification.

We can first observe that $\tau_b$ has a dramatic impact on the location error, under all configurations. As the LA computes the location error every second, $\tau_b$ values larger than one second result in missing position information and trigger the estimation process of missing intermediate locations presented in Sec. 4.4. Clearly, the longer the $\tau_b$, the more

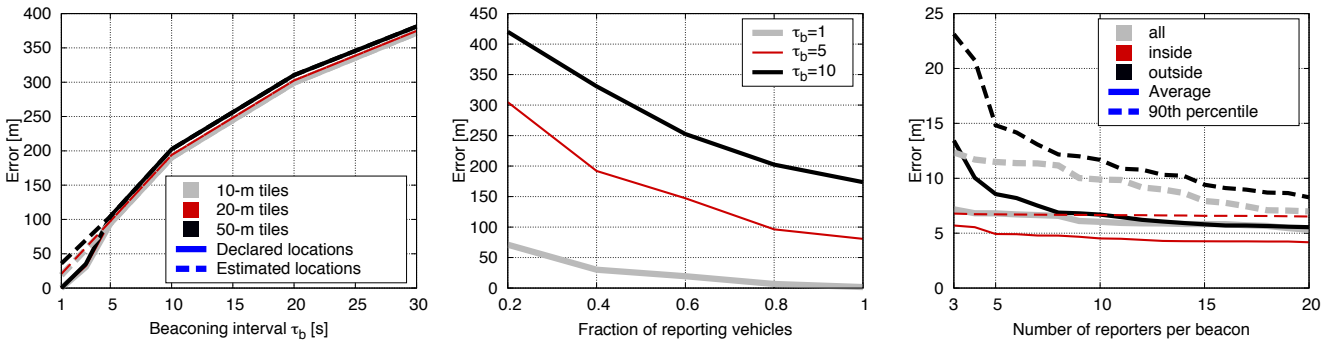



Fig. 6. Simulation: location error vs. (a) the beaconing interval $\tau_b$, (b) the fraction of reporting vehicles, and (c) the number of reporters per beacon when $\tau_b = 10$ s. Grey/red/black colors identify different tile sizes in (a) and reporter positions in (c); solid/dashed lines refer to declared/estimated locations in (a) and to average/90th percentile in (c).

distant the position samples, leading to a less accurate estimation of intermediate locations. When this effect is marginal ($\tau_b$ is between 1 and 3 seconds), the error ranges in the order of the tile size.

When comparing the errors yielded by declared and estimated positions, they only differ when the absolute error is small, and, even then, the distance between the two is always in the order of the tile size. This allows us to conclude that reports are an efficient source of information to estimate the actual location of vehicles, and that we can trust the $Q$-aware cooperative position identification in case no positioning information is explicitly provided by a vehicle.

Fig. 6(b) shows the impact of the fraction of vehicles participating in the A-VIP reporting, when the tile size is set to 10 m. When all vehicles upload report messages, i.e., the fraction is equal to 1, the error corresponds to that measured in Fig. 6(a). However, as participation in reporting dwindles, i.e., for lower values on the x axis, the error tends to grow, slowly at first and faster later on. This effect, consistent through all values of $\tau_b$, is due to the fact that, in presence of smaller sets of reporting vehicles, beacons are less likely to be received by any reporter. Non-reported beacons will never reach the LA. The latter will treat these situations as missing position information cases, thus estimating the location of vehicles whose beacons have not been reported as from Sec. 4.4. As discussed before, the estimate accuracy decreases as more beacons remain unreported. However, A-VIP appears robust to the lack of reporting, as errors become significant only if the majority of vehicles do not upload reports.

Fig. 6(c) shows a breakdown of the location error depending on the number and position of the reporters, for a tile size of 10 m and $\tau_b$ = 10 s. The overall average error (solid grey line) is not affected by the number of vehicles reporting the beacon, while the 90th percentile (dashed grey line) is. This implies that a low number of reporters can generate a few large error situations, namely, when beaconers fall outside the polygon whose vertices are the reporting vehicles (black solid and dashed lines). Conversely, if the beaconer is within such a polygon (red solid and dashed lines), the error remains low even for a small number of reporters. Indeed, in the latter case and when the reporters $v_j \in \mathcal{R}_i$ of a beacon from $v_i$ are farther apart, the intersection of the sets $\mathcal{S}_i^{(j)}$ is smaller, as shown in Fig. 2, and the location estimate is much more accurate. We can conclude that large position estimation errors only concern vehicles whose beacons are reported by a few neighbors clustered on one side of the beaconer.

**Testbed**. A direct comparison of testbed and simulation results is not viable due to the very different settings that characterize the two environments, including the covered area, the number of cars and the propagation conditions. However, the qualitative behavior of the location error versus the beaconing interval $\tau_b$ observed in the experimental evaluation, in Fig. 7(a), matches the simulated one in Fig. 6(a). Also in the testbed case, longer time intervals between back-to-back beacon transmissions determine higher location errors. The reason lies again in the difficulty of inferring intermediate locations between distant position samples.

We consider the match above as a positive result implying that real-world RF signal propagation, despite its complex and time-varying nature, does not induce dramatic errors in the A-VIP position estimation process. Similarly, real-world beacon and report message losses, measured to affect around 1% of messages in our experiments, do not impair the verification process at the LA. As a consequence, the experimental curves confirm that location errors in the order of the tile size (set to 10 m in these tests) are achievable in real settings if $\tau_b$ = 1 s.

Interestingly, the testbed results obtained with a varying number of vehicles (ranging from 1 to 5 and mapping onto different lines in Fig. 7(a)) also validate the finding that the error is significantly reduced when the number of vehicles (hence reporters) increases up to 5.

Finally, the testbed also gave us the possibility to assess the impact that the vehicle speed and geographical position have on the $Q$-aware estimation accuracy. Fig. 7(b) presents the relationship between the error on the estimated locations and the vehicle speed averaged over 30 s-intervals, when 5 vehicles are used and $\tau_b$ = 1 s. The vehicle speed is

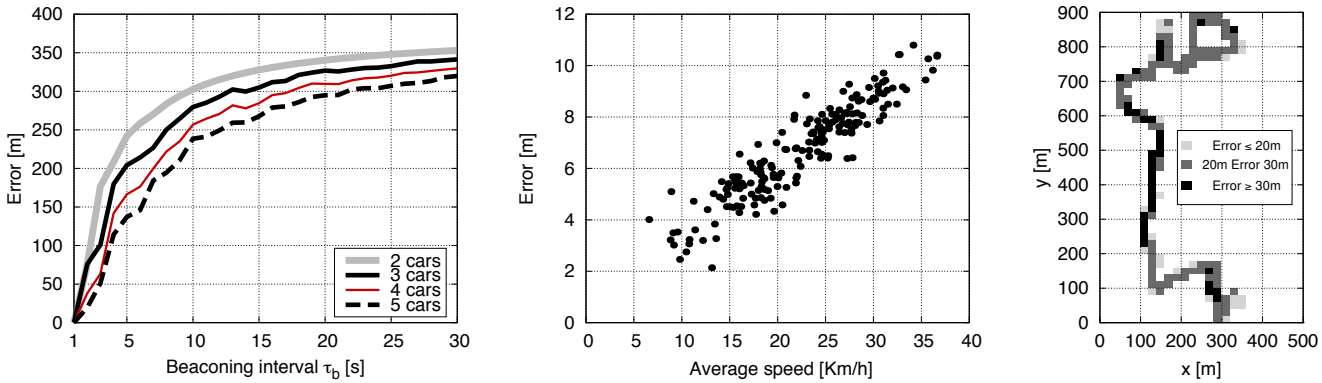



Fig. 7. Testbed: location error vs. (a) the beaconing interval, (b) the vehicle speed, and (c) the vehicle geographical position. The latter two plots show the error on the $Q$-aware estimation when $\tau_b = 1$ s and $\tau_b = 10$ s, respectively.

averaged so as to remove outliers due to GPS errors, hence make the plot more readable. The results show a strong correlation between the error on the estimated locations and the traveling speed, explained by the fact that higher speeds introduce a higher variability in vehicle positions and make the estimation less accurate. The geographical analysis of the error, depicted in Fig. 7(c) for $\tau_b$ = 10 s, is consistent with such a conclusion. Indeed, high errors (i.e., dark regions in the plot) are recorded on straight segments of the road when the speed is higher, while the lowest errors (i.e., light dots in the plot) are observed at slow-speed turns. Overall, we conclude that the $Q$-aware position estimation run by A-VIP yields good performance as confirmed by both simulation and real-world experiments.

### 6.3 Robustness to attacks

Having assessed A-VIP position estimation reliability in presence of correct nodes only, we now evaluate the robustness of our solution (described in Secs. 4.2–4.4) to attacks led by adversarial nodes. We consider attacks for which tamper-proof HSM is not needed. Consistently with the findings in Sec. 6.2 and if not stated otherwise, we will assume $\tau_b$ = 1 s, a tile side of 10 m, and all vehicles participating in the reporting process.

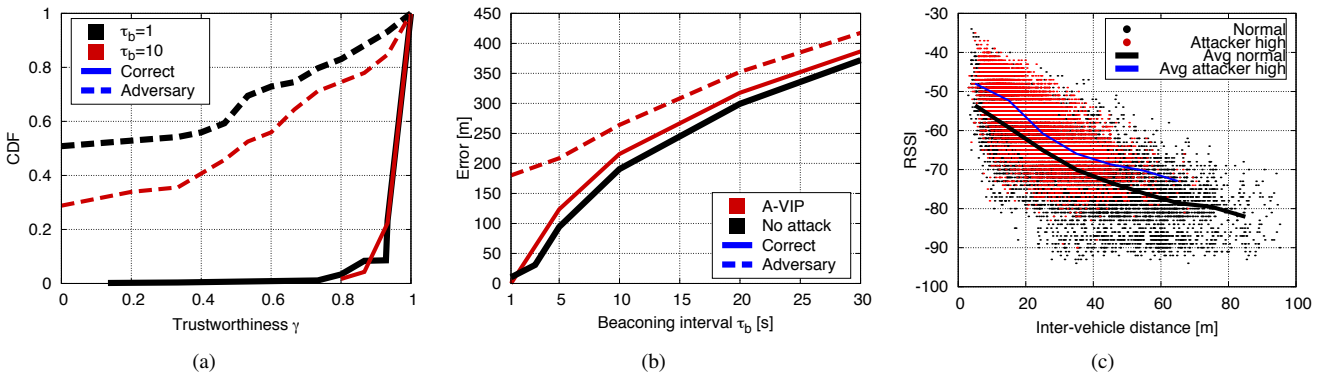
**Transmit-power attack**. We consider the case of transmit-power attacks, described in Sec. 5, and assess the A-VIP robustness via simulation. Fig. 8(a) shows the Cumulative Distribution Function (CDF) of the trustworthiness $\gamma$ assigned by A-VIP to correct (solid line) and adversarial (dashed line) vehicles. Different colors map onto beaconing intervals $\tau_b$ of 1 and 10 seconds, respectively. The distributions clearly show how A-VIP can tell apart correct and misbehaving nodes, assigning high $\gamma$ values (typically close to one) to the former, and much lower $\gamma$ values (often near zero) to the latter. Notably, the percentage of adversarial nodes with high trustworthiness is small, a good performance in light of the large percentage of attackers (10% as mentioned in Sec. 6.1) and the fact that they are allowed significant freedom, being able to increase their transmit power by up to 20 dB (100 mW).

The value of $\gamma$ allows the LA to decide which vehicles can be trusted and which cannot, as detailed in Sec. 4.4. The impact of such a classification on the accuracy of positions validated by the LA is portrayed in Fig. 8(b), in terms of the resulting location error. We can observe that correct vehicles are effectively identified by A-VIP: their errors with (solid red line, "A-VIP correct") or without (solid black line, "No attack") adversaries mostly overlap, and they do not suffer from the presence of transmit-power attackers. On the contrary, attackers are tracked down by A-VIP: their actual locations are estimated by the LA (dashed red line, "A-VIP adversary") with fair accuracy.

We attempted running transmit-power attacks in the experimental testbeds as well. However, the wireless interface cards we employed only allow for very limited transmission power variations, of 5 dB at most. As shown in Fig. 8(c), such a small power offset is lost in the Received Signal Strength Indicator (RSSI) variability due to normal RF signal propagation phenomena. Therefore, the interface card limitations did not allow us to implement adversarial nodes that were substantially different from correct vehicles in terms of transmitted power.

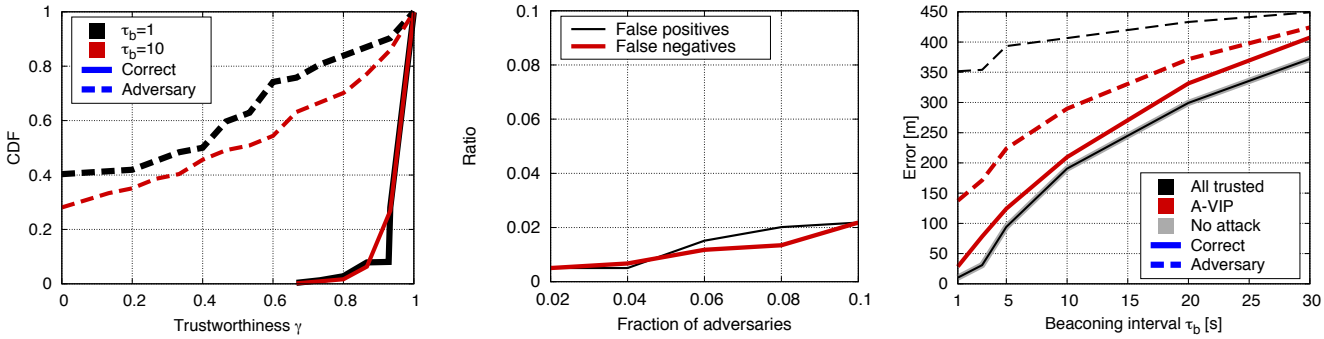
**False location attack**. As described in Sec. 5, false location attacks are performed in our evaluation by announcing outdated positions along with consistent cryptographic material. We first study their effect in simulation, assuming that adversaries run false location attacks by including in their beacons the position they were at 10 s before.

Fig. 9(a) portrays the CDF of the trustworthiness probability $\gamma$ for correct and adversarial vehicles, when $\tau_b$ is set to 1 s and 10 s. Also in this case, A-VIP reliably separates the two classes of nodes, assigning high $\gamma$ values to the former and low $\gamma$ values to the latter. Only 5% to 10% of the attackers are assigned a high trustworthiness, and this mainly occurs for adversarial nodes that did not move significantly during the 10-second delay of the attack. The proper classification of correct and adversarial behaviors leads to extremely low false positives (i.e., attackers tagged as trustworthy) and false negatives (i.e., correct nodes tagged as adversarial). Fig. 9(b) depicts false positives and false negatives as the fraction




(a) (b) (c)

Fig. 8. Transmit-power attack. (a) Simulation: distribution of trustworthiness probability $\gamma$. (b) Simulation: location error vs. beaconing interval $\tau_b$. (c) Testbed: RSSI vs. communication distance for normal and attacker users. In (a) and (b) solid/dashed curves indicate correct/adversary nodes. Black/red colors identify different $\tau_b$ in (a), while they differentiate the "A-VIP" and the "No attack" cases in (b).




(a) (b) (c)

Fig. 9. False location attack with 10 s-old positions. Simulation: (a) distribution of the trustworthiness probability $\gamma$, for a 10% of adversaries; (b) false positives and negatives vs. fraction of attackers when $\tau_b = 10$ s; (c) location error vs. beaconing interval $\tau_b$, for a 10% of adversaries. In (a) and (c), solid/dashed curves indicate correct/adversary nodes. In (a) black/red colors identify different $\tau_b$, while in (c) black/red/grey colors identify the "All trusted", "A-VIP" and "No attack" cases. In (c), in the "No attack" case, all vehicles are correct, thus only the "Correct" curve appears.

of adversaries varies between 2% and 10%. The results are obtained for $\tau_b = 10$ s and shows that both types of incorrect tagging are limited to less than 2% of vehicles in all cases.

Similarly, the good classification performance of A-VIP leads to limited location errors, in Fig. 9(c). Once more, longer beaconing intervals result in higher location errors, for all cases. However, differences emerge when we focus on different curves. When all nodes are correct and we do not have any attack (solid grey line, "No attack"), we have the standard position estimation error already discussed in Sec. 6.2. By introducing a 10% of attackers (red lines), we observe that the location error of correct nodes (solid red line, "A-VIP correct") – properly identified by A-VIP as previously shown – does not change significantly. Positions announced by adversarial nodes are discarded: their actual locations, estimated through the cooperative $Q$-aware technique (dashed red line, "A-VIP adversary"), show again a fair accuracy. For completeness, the plot also shows the error values in the case where all nodes are trusted (black lines). We note that correct nodes (solid black line, "All trusted correct") exhibit the minimum error, since the position they advertise is trusted by the LA and matches their actual location. However, the LA believes also adversarial vehicles (dashed black line, "All trusted adversary"), which leads to a very high error in their position.

Fig. 10 shows the resilience of A-VIP to delay attacks through the measured location error for $\tau_b = 1$ s and a delay of 10 s or 30 s. Each pair of bars refers to one of the cases plotted in Fig. 9(c) and, for sake of readability, the numerical value of the error (expressed in meters) is reported on top of each bar. We note that a delay of 10 s allows attackers to correctly announce positions that are up to 60 m away if the trustworthiness mechanism of A-VIP is not used ($2^{nd}$ grey bar from the left, "All trusted adversary"). When such a mechanism is employed, the error ($4^{th}$ grey bar from the left, "A-VIP adversary") becomes negligible, meaning that adversaries are correctly identified and their actual locations are estimated within the accuracy limits of the $Q$-aware technique.

Increasing the attack delay to 30 s leave more room for

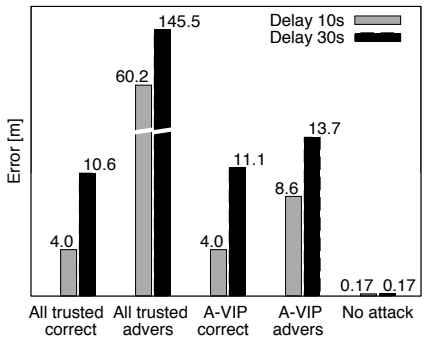



Fig. 10. False location attack. Testbed (2 attackers out of 5 vehicles): location error for $\tau_b = 1$ s and when the announced position is 10 s or 30 s old.

misbehavior. We observe that without verification, adversarial vehicles can announce positions almost 150 m away from their actual location ($2^{nd}$ black bar from the left, "All trusted adversary"). Instead, the trustworthiness mechanism of A-VIP still allows us to reliably tell apart incorrect nodes. Their true position is estimated with an error in the order of meters ($4^{th}$ black bar from the left, "A-VIP adversary") with respect to the case where attackers are absent ($5^{th}$ black bar from the left, "No attack").

**Sybil attack**. The last type of threat considered in our performance evaluation is the one brought about by the Sybil attack, detailed in Sec. 5. The limited number of vehicles available in our testbed does not allow us to experimentally evaluate A-VIP resilience to Sybil attacks. Therefore, in the following we resort to simulation. More precisely, we consider that 2% to 10% of the vehicles run Sybil attacks, and set the $f$ parameter of the A-VIP buddy detection mechanism presented in Sec. 4.3 to 0.05. As shown by the results below, this low fraction is already sufficient to detect Sybil attacks in most cases.

We first consider the case where adversarial nodes own cryptographic material granting them one additional identity. Indeed, this is barely sufficient for attackers to pass A-VIP verification even when no buddy detection is used. As shown in Fig. 11(a), false positives and negatives remain below 7% in all cases (dashed lines), as self-reporting via one additional identity is not sufficient to overcome the honest reporting by correct nodes. At any rate, the buddy detection mechanism (solid lines) greatly impairs the success probability of Sybil attacks as well as the chances of misclassifying correct vehicles. Fig. 11(b) shows that adversaries can modify their location by several hundred meters, when no verification is run (dashed black line) as well as when no buddy detection is used (dashed red line). By employing A-VIP with buddy detection, no maneuvering room is left to Sybil attackers: they are identified and their actual location is accurately estimated (dashed grey line).

Adversaries capable of impersonating three vehicles in addition to their actual identity make a great case for a solution such as A-VIP. Fig. 11(c) proves that three illicitly owned identities are sufficient to grant a Sybil attacker significant probability of success. Specifically, more than 20% of the attacks (dashed red line) are successful if no buddy detection is employed. As a side effect, up to 14% of correct vehicles (dashed black line) are at risk of being tagged as untrustworthy. The adoption of the buddy detection mechanism however limits both false negatives and positives to values below 2% in the worst case (solid lines).

The positive impact of the buddy detection naturally translates into much lower location errors, shown in Fig. 11(d). With three additional identities, Sybil attackers can modify their location by more than 600 m without being detected by the LA, if no A-VIP trustworthiness mechanism (dashed black line) or buddy detection (dashed red line) are employed. Conversely, A-VIP with buddy detection bounds the error to nearly zero values.

## 7 Conclusions

We presented A-VIP, a lightweight privacy-preserving framework for verification and inference of vehicle positions by a Location Authority. A-VIP leverages computationally-inexpensive symmetric cryptography and reciprocal reporting of anonymized beacons by vehicles. Simulation and experiments in real-world testbeds have shown A-VIP capable of achieving its goals in both dense and sparse vehicular settings. Our results also show that A-VIP can effectively cope with several feasible attacks on a position verification system, with a small percentage of false positive/negatives.

## Acknowledgment

We thank Prof. Falko Dressler and Dr. Christoph Sommer for providing us with the Ingolstadt mobility trace.

## References

[1] Thales ISS, Thales, Jan. 2011 [Accessed on July 2012].
[2] B. Wiedersheim *et al.*, "Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change Is not Enough," *IEEE WONS*, 2010.
[3] E. Schoch, F. Kargl, "On the Efficiency of Secure Beaconing in VANETs," *ACM WiSec*, 2010.
[4] IEEE 1609.2 Standard for Wireless Access in Vehicular Environments Ñ Security Services for Applications and Management Messages, 2013.
[5] J. Hwang, T. He, Y. Kim, "Detecting Phantom Nodes in Wireless Sensor Networks," *IEEE Infocom*, Anchorage, AK, May 2007.
[6] E. Ekici, S. Vural, J. McNair, D. Al-Abri, "Secure Probabilistic Location Verification in Randomly Deployed Wireless Sensor Networks," *Elsevier Ad Hoc Networks*, vol. 6, no. 2, pp. 195-209, 2008.
[7] S. Čapkun, K. Rasmussen, M. Cagalj, M. Srivastava, "Secure Location Verification with Hidden and Mobile Base Stations," *IEEE Trans. on Mobile Computing*, vol. 7, no. 4, pp. 470–483, 2008.
[8] J. Chiang, J. Haas, Y. Hu, "Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration," *ACM WiSec*, Zurich, Switzerland, Mar. 2009.
[9] T. Leinmüller, C. Maihöfer, E. Schoch, F. Kargl, "Improved security in geographic ad hoc routing through autonomous position verification," *ACM VANET*, Los Angeles, CA, Sept. 2006.
[10] T. Leinmüller, E. Schoch, F. Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks," *IEEE Wireless Communications*, pp. 15–21, Oct. 2006.
[11] J.-H. Song, V. Wong, V. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks," *IEEE Globecom*, New Orleans, LO, Dec. 2008.

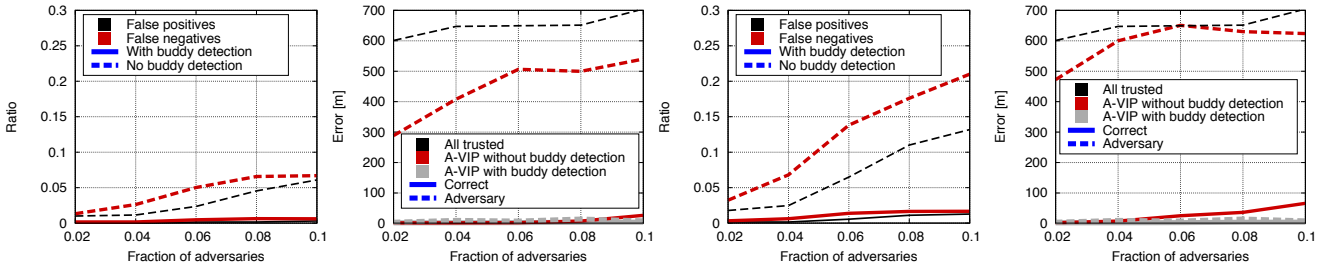



Fig. 11. Sybil attack. Simulation: adversaries own one additional identity ((a), (b)) and three additional identities ((c), (d)). (a) and (c): False positives and negatives vs. fraction of attackers. (b) and (d): Location error vs. fraction of attackers. Curves are differentiated by the combination of color and line pattern. In (a) and (c), black/red colors indicate false positives/negatives, and solid/dashed lines the presence/absence of buddy detection. In (b) and (d), black/red/grey colors identify the cases where all nodes are trusted or A-VIP is used without/with buddy detection, while solid/dashed curves map onto correct/adversary nodes.


[12] M. Fiore, C. Casetti, C.-F. Chiasserini, P. Papadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, 2013.

[13] M. Abu-Elkheir, S.A. Hamid, H.S. Hassanein, I.M. Elhenawy, S. Elmougy, "Position verification for vehicular networks via analyzing two-hop neighbors information," *IEEE LCN On-Move*, Bonn, Germany, Oct. 2011.

[14] O. Abumansoor, A. Boukerche, "A secure Cooperative Approach for Non line-of-Sight Location Verification in VANET," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 275–285, 2012.

[15] Z. Ren, W. Li, Q. Yang, "Location Verification for VANETs Routing," *IEEE WiMob*, Marrakech, Morocco, Oct. 2009.

[16] X. Xue, N. Lin, J. Ding, Y. Ji, "A trusted neighbor table based location verification for VANET routing," *IET ICWMMN*, Beijing, China, Jan. 2010.

[17] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communication Systems: Design and Architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[18] K. Sampigethaya, M. Li, L. Huang, R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," *IEEE JSAC*, vol.25, no.8, pp.1569–1589, Oct. 2007

[19] D. Eckhoff, C. Sommer, T. Ganseny, R. German, F. Dressler, "Strong and Affordable Location Privacy in VANETs: Identity Diffusion Using Time-Slots and Swapping," *IEEE VNC*, 2010.

[20] W. Diffie, M. Hellman, "Privacy and Authentication: An Introduction to Cryptography," *Proceedings of the IEEE*, vol. 67, no. 3, pp. 397–427, Mar. 1979.

[21] F. Klingler, F. Dressler, J. Cao, C. Sommer, "Use Both Lanes: Multi-channel Beaconing for Message Dissemination in Vehicular Networks," *WONS,* 2013.

[22] C. Sommer, D. Eckhoff, R. German, F. Dressler, "A Computationally Inexpensive Empirical Model of IEEE 802.11p Radio Shadowing in Urban Environments," *IEEE WONS*, 2011.

[23] S.P. Boyd, L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[24] S. Chang, Y. Qi, Ho. Zhu, J. Zhao, X. Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks," *IEEE Trans. on Paralled and Distributed Systems*, vol. 23, no. 6, pp. 1103–1114, Jun. 2012.


**Francesco Malandrino** (S'10, M'13) graduated (summa cum laude) in Computer Engineering from Politecnico di Torino in 2008. He received his PhD from Politecnico di Torino in 2011. In 2010–2011 he has been a visiting researcher at University of California at Irvine. His interests focus on wireless and vehicular networks and infrastructure management.

**Carlo Borgiattino** (S'12) graduated (summa cum laude) in Telecommunication Engineering from Politecnico di Torino in 2011. In 2012, he joined the Department of Electronics and Telecommunications of Politecnico di Torino as a Ph.D student. His research activities are focused on vehicular and wireless mesh networks.

**Claudio Casetti** (M'05) graduated from Politecnico di Torino in 1992 and received his PhD in Electronic Engineering from the same institution in 1997. He is an Assistant Professor at Politecnico di Torino. He has coauthored more than 130 papers in the fields of networking and holds three patents.

**Carla-Fabiana Chiasserini** (M'98, SM'09) received her Ph.D. in 2000 from Politecnico di Torino, where she is currently an Associate Professor. Her research interests include protocols and performance analysis of wireless networks. Dr. Chiasserini has published over 200 papers at major venues, and serves as Associated Editor of several journals.

**Marco Fiore** (S'05, M'09) is a researcher at CNR–IEIIT, Italy, and at INRIA within the UrbaNet team hosted by the CITI Lab of INSA Lyon, France. He received M.Sc degrees from the University of Illinois at Chicago and Politecnico di Torino, in 2003 and 2004, respectively, and a PhD degree from Politecnico di Torino, in 2008. His research interests are in the field of mobile and vehicular networking.

**Roberto Sadao** graduated from Universidade de São Paulo (USP), Brazil, in 2009, where his currently a PhD student. He has been a visiting PhD student at Politecnico di Torino, Italy His research interests are in the field of mobile computing, context-aware systems and IP connectivity management.