



## Detecting Sybil attacks in VANETs



Bo Yu<sup>a,\*</sup>, Cheng-Zhong Xu<sup>a</sup>, Bin Xiao<sup>b</sup>

<sup>a</sup> Department of Electrical and Computer Engineering, Wayne State University, USA

<sup>b</sup> Department of Computing, Hong Kong Polytechnic University, Hong Kong

### ARTICLE INFO

#### Article history:

Received 8 February 2012

Received in revised form

16 October 2012

Accepted 1 February 2013

Available online 9 February 2013

#### Keywords:

Sybil attacks

VANET

Position verification

### ABSTRACT

Sybil attacks have been regarded as a serious security threat to Ad hoc Networks and Sensor Networks. They may also impair the potential applications in Vehicular Ad hoc Networks (VANETs) by creating an illusion of traffic congestion. In this paper, we make various attempts to explore the feasibility of detecting Sybil attacks by analyzing signal strength distribution. First, we propose a cooperative method to verify the positions of potential Sybil nodes. We use a Random Sample Consensus (RANSAC)-based algorithm to make this cooperative method more robust against outlier data fabricated by Sybil nodes. However, several inherent drawbacks of this cooperative method prompt us to explore additional approaches. We introduce a statistical method and design a system which is able to verify where a vehicle comes from. The system is termed the Presence Evidence System (PES). With PES, we are able to enhance the detection accuracy using statistical analysis over an observation period. Finally, based on realistic US maps and traffic models, we conducted simulations to evaluate the feasibility and efficiency of our methods. Our scheme proves to be an economical approach to suppressing Sybil attacks without extra support from specific positioning hardware.

© 2013 Elsevier Inc. All rights reserved.

### 1. Introduction

Until recently, road vehicles were the realm of mechanical engineers. However, with the plummeting costs of electronic components and the permanent willingness of the manufacturers to increase road safety and to differentiate themselves from their competitors, vehicles are becoming “computers on wheels”, or rather “computer networks on wheels” [22]. Vehicular Ad hoc Networks (VANETs) have the potential to not only facilitate the decision making tasks of the drivers (e.g., trip planning based on traffic congestion on the road), but also to improve highway safety (by bringing information about catastrophic events and road conditions to the driver’s attention). However, researchers [20,22] have pointed out that VANETs are facing a number of security threats, which may impair the efficiency of VANETs and even life safety. One of these threats is Sybil attacks, in which a malicious vehicle claims multiple fabricated identities. Sybil attacks can be harmful to a variety of VANET applications. For example, a greedy driver can fabricate that a number of vehicles are traveling nearby, which creates an illusion of traffic congestion. Then, other vehicles will choose an alternate route and evacuate the road for the greedy driver. Since the fabricated vehicles are actually under the control

of one malicious node, the malicious node may have further control of other network protocols. For example, the large amount of Sybil nodes may deviate the results of voting-based protocols from the truth; the Sybil nodes may also launch Denial of Service (DoS) attacks to impair the normal operations of data dissemination protocols, such as [27,29,13]. Sybil attacks may even cause serious safety threats. For example, in the application of deceleration warning systems [20], if a vehicle reduces its speed significantly, it will broadcast a warning to the following vehicles. Recipients will relay the message to vehicles further behind. However, this forwarding process can be intervened by a large number of malicious Sybil vehicles. In this way, the malicious adversary can create a massive pileup on the highway, potentially causing great loss of life.

Traditionally in Ad hoc Networks and Sensor Networks, three types of defense against Sybil attacks are introduced, including: radio resource testing, identity registration, and position verification [9]. Radio resource testing is based on the assumption that a radio cannot send or receive simultaneously on more than one channel. It does not apply to VANETs since a greedy driver may cheaply acquire multiple radios. Identity registration alone cannot prevent Sybil attacks, because a malicious node may get multiple identities by non-technical means such as stealing. Further, strict registration causes serious privacy concerns. In position verification, the network verifies the position of each node and ensures that each physical node is bound with only one identity. A number of position (or distance) verification techniques [3,1,24,4] have been proposed recently. However, they either are designed

\* Corresponding author.

E-mail addresses: [boyu@wayne.edu](mailto:boyu@wayne.edu) (B. Yu), [czxu@wayne.edu](mailto:czxu@wayne.edu) (C.-Z. Xu), [csbxiao@comp.polyu.edu.hk](mailto:csbxiao@comp.polyu.edu.hk) (B. Xiao).

for indoor applications or rely on stationary base stations or specific hardware. None of them would be suitable for the highly mobile context of vehicular networks.

The motivation behind this paper is that we can estimate a node's position by analyzing its signal strength distribution and then verify whether its position claim is consistent with the estimated position. In traditional sensor networks, we cannot rely on signal-strength-based position verification for two reasons. First, since sensor nodes are static, we can only obtain a static pattern of signal strength distribution and the accuracy is limited. We cannot distinguish two physical nodes which are close to each other either. Second, it is difficult to ensure that the position estimation process is not intervened by potential Sybil nodes. However, the unique properties of VANETs present us more opportunities to address the problem from a different perspective. For example, we can take advantage of the highly mobile context of VANETs to accumulate more signal strength measurements.

In this paper, we study the feasibility of using signal strength distribution analysis to detect Sybil attacks. First, we design a cooperative detection method, in which multiple neighboring nodes cooperate to measure the signal strength distribution of a suspicious node and verify the physical position of the suspicious node. We use a Random Sample Consensus (RANSAC)-based algorithm to increase the estimation robustness against outlier data fabricated by Sybil nodes. However, our simulation results illustrate that given the unstable nature of radio propagation, this basic cooperative method can only afford quite limited accuracy. Moreover, it is still vulnerable to fabricated measurements by Sybil nodes. To make this cooperative method apply to VANETs, one essential step is to ensure that all signal strength measurements originate from honest physical nodes instead of fabricated Sybil nodes. To solve this problem, we propose the concept of Presence Evidence System (PES). With this system, we can ensure that nodes in the opposite traffic are physical nodes and we can have them as the trustworthy sources of signal strength measurements. This system takes full advantage of the inherent properties of VANETs such as high mobility, road topology, as well as indirect support from roadside infrastructure. From another aspect, we find that we can accumulate more signal strength measurements by extending the observation period, therefore improving the detection accuracy. Led by this inspiration, we present a statistical detection method. The statistical method performs hypothesis tests on accumulated measurements, and tries to judge whether the measurements match a normal distribution pattern. A Sybil node is reported if its distribution pattern is inconsistent with its claimed physical position. We used simulations to evaluate the performance of our final scheme. The simulations are based on realistic US maps and traffic models. Our scheme proves to be an economical and efficient way to suppress Sybil attacks without the requirements of specific positioning hardware.

The rest of this paper is organized as follows. We introduce the related work in Section 2. In Section 3, we define the attack model and system assumptions. Section 4 presents the cooperative detection method based on analysis of signal strength distribution. Section 5 introduces the concept of Presence Evidence System. Section 6 proposes the statistical detection method to detect potential Sybil nodes. Section 7 introduces the final integrated scheme. Section 8 evaluates our scheme by simulations based on realistic US maps and traffic models. Section 9 discusses several related problems and summarizes several unique features of our scheme. Finally, we conclude the paper in Section 10.

## 2. Related work

Considerable attention from academia has been attracted by emerging Vehicular Networks. There have been a few proposals pointing out the importance of security in Vehicular Networks

[2,20,22,12]. In [20,22,23], a common security threat of Sybil attacks is introduced. In this attack, multiple identities are claimed by a single malicious node with fabricated positions.

Sybil attacks are quite harmful for a variety of network applications. Basically, in VANETs, Sybil attacks may easily create an illusion of traffic congestion. What is more, Sybil attacks may have a major impact on other existing VANET protocols, including MAC layer, routing layer, as well as application layer. For example, in the literature, the multi-hop broadcast protocol [13], the reliable MAC protocol [27], the bandwidth sharing protocol [25], and the data dissemination protocol [29] are all subject to Sybil attacks, because they all rely on nodes' cooperation to forward packets and a malicious node may easily crack them by using its large number of fake nodes.

Efforts have been made to detect Sybil nodes in Mobile Ad hoc Networks and Sensor Networks. Newsome et al. [17] introduced several techniques to detect Sybil attacks in ad hoc networks, including radio resource testing, identity registration, and position verification. Whereas radio resource testing relies on specific assumptions on radio modules and identity registration alone is not effective enough, position verification comes to be a more promising approach for vehicular networks. The use of received radio signal strength for positioning was proposed in [1]. It is designed for indoor applications, relying on establishing a signal-strength-distribution map in advance. Demirbas et al. [5] introduced an RSSI-based scheme for detecting Sybil attacks for resource-poor sensor networks. The scheme takes advantage of statistical RSSI readings in a stationary sensor network. Brands et al. [3] proposed a distance bounding protocol that can be used to verify the proximity of two devices connected by a wired link. Sastry et al. [24] proposed a new distance bounding protocol, based on ultrasound and radio wireless communication. The protocol can only make a rough decision about whether or not a claimer is within a certain region. Capkun et al. [4] presented a secure positioning scheme, which relies on multiple base stations as reference points and supposes that nodes are static. These schemes do not fit the highly mobile context of VANETs.

Most recently, the detection of Sybil attacks has also been studied in the field of Vehicular Networks. Golle [9] presented a security framework which enables nodes to verify the validity of the received data based on neighborhood observations. The scheme focused on the reasoning of conflicting observations, but simply assumed the nodes' capability of detecting the distances to other nodes or the precise locations of other nodes, which is exactly the issue we studied in this work. Leinmuller et al. [14] used a set of thresholds to verify a single node's position claims. It is an effective method to limit the range of a single node's bogus position claims, whereas our study deals with multiple nodes' (multiple Sybils') bogus position claims. Especially, the Mobility Grade Threshold introduced in [14] may not be efficient in case of multiple Sybil nodes where each Sybil node holds in a relatively constant position. Yan et al. [28] introduced several useful methods to verify the locations of neighboring vehicles with the help of on-board radars. The authors alleviated the line-of-sight limitation of a radar by using a collaborative method. A Sybil attack detection scheme based on roadside unit support was proposed in [19]; in this scheme, a vehicle collects certified time stamps from roadside units as it is running, and two nearby vehicles cannot have exactly the same series of time stamps, otherwise they are Sybil nodes. The scheme relies on a dense deployment of roadside units. Ghosh et al. [8] discussed the misbehavior detection from the application layer. The authors proposed a root-tree approach to achieve misbehavior detection and identify the root cause. Above works use various methods from different layers to detect attacks in VANET, but meanwhile all have certain limitations. Sybil attacks remain to be an open issue in the field of Vehicular Networks. The proposed scheme in this paper will serve as a supplementary approach to suppressing Sybil attacks in an economic way without the requirement for specific hardware.

### 3. Attack model and assumptions

In this section, we define the attack model of Sybil attacks and then present the system assumptions which our study is based on.

#### 3.1. Attack model

Sybil attacks refer to a malicious node illegitimately taking on multiple identities [17]. In wireless networks, mobile nodes usually discover new neighbors by periodically broadcasting beacon packets, in which they claim their identities and positions. However, given the invisible nature of wireless communication, a malicious node can easily claim multiple identities without being detected. Identity authentication does not help prevent Sybil attacks in VANETs, since a malicious driver can still get additional identity information by non-technical means such as stealing, or simply borrowing from his friends. The goal of detecting Sybil attacks is to ensure that each physical node is bound with only one legal identity.

In this paper, we refer to a vehicle as a node in the context of VANETs. We refer to a physical node claiming multiple identities as a *malicious node* and, correspondingly, the malicious node's fabricated identities as *Sybil nodes*.

#### 3.2. Assumptions

Our study on Sybil attacks are based on the following assumptions. First, we focus on the most basic Sybil-attack threat, which is caused by individual greedy drivers (vehicles). We assume that most other drivers (vehicles) can be trusted. We do not consider cooperative Sybil attacks, in which multiple malicious vehicles cooperate to launch Sybil attacks. Second, all the vehicles, including greedy drivers' vehicles, are equipped with the same radio module. The radio module may be based on any Radio Frequency (RF) communication technique providing Received Signal Strength Indicator (RSSI), such as DSRC [6]. Third, we assume that each vehicle is equipped with GPS devices and digital maps. GPS positions are supposed to be accurate. Finally, we assume that roadside base stations are sparsely deployed along roads, and the identity authentication infrastructure such as an Electronic License Plate (ELP) [12] has been implemented for the whole network. Identity authentication prevents a malicious vehicle from unlimitedly fabricating false identities. Of course, as we mentioned before, identity authentication alone cannot prevent Sybil attacks. Since roadside base stations are sparsely deployed and the majority of road sections are not covered by roadside base stations, we do not rely on direct support from roadside stations.

### 4. Cooperative detection method

Traditionally, the detection of Sybil attacks usually relies on three categories of approaches, namely radio resource testing, identity registration, and position verification [17,9]. Radio resource testing requires special radio modules such as multi-channel radio and identity registration alone does not work very well in VANETs. Therefore, position verification is regarded as a more promising approach for VANETs.

In this section, we propose a cooperative detection method for verifying position claims by signal strength analysis. We design a RANSAC (Random Sample Consensus)-based algorithm to improve the robustness in estimating positions. We also explore the feasibility of this cooperative method through simulations.

#### 4.1. Cooperative method

The cooperative detection method detects potential Sybil nodes by position verification, relying on monitoring the signal strength

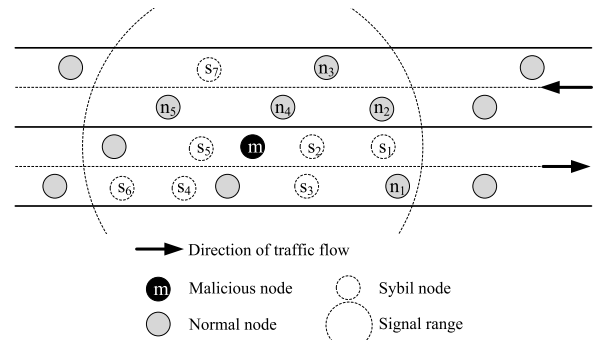


Fig. 1. An example VANET under Sybil attacks.

of periodical beacons. For clarity of description, we define three categories of nodes' roles: *claimer*, *witness*, and *verifier*. Each node would periodically play all these roles, that is, each node is a claimer, a witness as well as a verifier but at various moments and for various purposes.

1. *Claimer*. Each node periodically broadcasts a beacon message at *beacon intervals*,  $t_b$ , for the purpose of neighbor discovery. In the beacon message, it claims its identity and position such as GPS position. At this moment, we name the node as a claimer. The goal of our method is to verify its claimed position.

2. *Witness*. All neighboring nodes, within the signal range of the claimer, would receive the previous beacon message. They measure the signal strength and save the corresponding neighbor information in their memory. Next time they broadcast a beacon message, they will attach their neighbor list, including the signal strength measurements for each received beacon, to the beacon message. We name these nodes performing measurements and reporting measurements as witnesses.

3. *Verifier*. We call a node performing position verification a verifier. After receiving a beacon message, a node waits for a *verifying interval*,  $t_v$ , during which it collects enough signal strength measurements concerning the previous beacon message from neighboring witnesses.  $t_v$  may be a little longer than the beacon interval  $t_b$ , since after another interval of  $t_b$ , each neighboring witness should have broadcasted a beacon containing the expected measurements. With the collected measurements, the node (verifier) can locally compute an estimated position of the claimer. Then, the node compares the estimated position with the previously-claimed position of the claimer. If the difference exceeds a predefined threshold  $\Theta$ , the claimer is regarded as a Sybil node.

We take Fig. 1 as an example. Node  $s_1$ , a claimer (a Sybil node), broadcasts a beacon, claiming its identity and position. Node  $n_1$ , a verifier, collects all signal strength measurements from neighboring witnesses which have received the beacon. Obviously, the final estimated position of  $s_1$  would be near the position of node  $m$ , instead of the position  $s_1$  claimed, as node  $s_1$  and  $m$  are physically the same vehicle.

The beacon message can be in the following format:

{NodeID, Beacon#, Position, NebList, Signature}  
NebList : {NodeID<sub>i</sub>, Beacon#<sub>i</sub>, RSSI<sub>i</sub>},

where NodeID is the claimer's identity, Beacon# is a beacon sequence number, Position is the sender-claimed position, NebList is the sender's most recent neighbor list containing signal strength measurements, Signature is the digital signature for the whole packet. In each item of NebList, RSSI<sub>i</sub> is the Received Signal Strength of beacon Beacon#<sub>i</sub> recently received from neighboring node NodeID<sub>i</sub>.

Therefore, the next step is to design a method to calculate the estimated position based on collected measurements.

## 4.2. Calculation of position estimation

In this subsection, we study the calculation of claimers' estimated positions. We first define the radio model and the corresponding signal strength distribution model, and then propose two methods to fit the model into collected measurements, which finally obtain the estimated position of a claimer.

**Radio model.** We apply a widely-used radio propagation model, the shadowing model [21], which consists of two parts. The first part is known as path loss model, which also predicts the mean received power at distance  $d$ . The second part of the shadowing model reflects the variation of the received power at a certain distance. The overall shadowing model is represented by

$$\left[ \frac{P_r(d)}{P_r(d_0)} \right]_{dB} = -10\beta \log \left( \frac{d}{d_0} \right) + X_{dB}, \quad (1)$$

where  $d_0$  is a reference position,  $d$  is the position where the signal strength is measured,  $\beta$  is called the path loss exponent, and  $X_{dB}$  is a Gaussian random variable with zero mean and standard deviation  $\sigma_{dB}$ .  $d_0$  and  $\beta$  are constants specified by radio modules and physical environments.

Measurements from a field test [16] suggest that signal attenuation can be well modeled using the shadowing model with a standard deviation of 9.43 dB and a low path loss exponent of  $n = 1.03$ , i.e.  $X_{dB} = 9.43$  and  $\beta = 1.03$  in our radio model.

**Signal strength distribution model.** Based on above radio propagation model, we define our signal-strength distribution model as follows:

$$\begin{aligned} RSSI_p(d) &= E \left( -10\beta \log \left( \frac{|d-p|}{d_0} \right) + X_{dB} \right) \\ &= -10\beta \log \left( \frac{|d-p|}{d_0} \right), \end{aligned} \quad (2)$$

where  $RSSI$  can be described as the expected (mean) signal strength at position  $d$  given signal source position  $p$ .  $p$  is the only varying parameter in this model, and we can fit the model into collected measurements by varying  $p$ . In other words, if  $p$  is given, a model is uniquely determined.

### 4.2.1. Basic MMSE-based calculation

To calculate the estimated position, one possible method is to perform Minimum Mean-Square Error (MMSE) on the collected signal strength readings and the signal strength distribution model.

To obtain the estimated position, we first calculate the mean square error:

$$MSE_p(s) = \frac{\sum_{i=1}^k (s(w_i) - RSSI_p(w_i))^2}{k}, \quad (3)$$

where  $p$  is a potential position of the claimer,  $k$  is the number of witnesses,  $s$  is the set of signal strength readings ( $s(w_i)$  indicates the signal strength reading at witness  $w_i$ ),  $RSSI_p(w_i)$  is the signal strength at  $w_i$  obtained from the signal strength distribution model. By varying  $p$ , we can minimize  $MSE$  and finally get the optimal estimated position  $\hat{p}$ . It is possible that the calculation may be trapped in a local minimum. We can use random reset to restart the calculation.

Actually, this basic approach is based on curve fitting, which finds a curve (a signal strength distribution model) which matches a series of data points. That is also to say, we can derive a model from a set of signal strength readings.

One obvious drawback may appear in this basic approach. Since signal strength readings are collected from witnesses, if witnesses are Sybil nodes, the readings from them cannot be trusted. The final

estimated position may be far deviated due to the untrustworthy readings from Sybil witnesses. Therefore, it is important to remove the outlier readings by the potential Sybil nodes.

In the next subsection, we investigate using an iterative method to reduce the impact of outlier readings.

### 4.2.2. RANSAC-based calculation

In this subsection, we propose a Random Sample Consensus (RANSAC)-based method to improve the robustness in estimating the position of a vehicle. RANSAC is proposed by A. Fischler et al. [7] and has been widely used in computer graphics, artificial intelligence, etc., to improve system robustness. We adopt it in the detection of potential Sybil vehicles.

---

#### Algorithm 1: RANSAC-based calculation

---

**Input:**  $n$  signal strength measurements and corresponding positions

**Output:** Estimated position of the subject

```

1  $S \leftarrow \emptyset$ ; //Set of consensus sets
2 while  $i \leq f$  do
3   //f is number_of_trials
4    $s \leftarrow \text{random}(b)$ ; //initialize a random consensus set of size  $b$ 
5   while  $\text{error}(s) \leq \gamma$  do
6      $r \leftarrow \arg \min_{r \in s} \{\text{error}(s + \{r\})\}$ ;
7      $s \leftarrow s + \{r\}$ ;
8   end
9    $s \leftarrow s - \{r\}$ ;
10   $S \leftarrow S + \{s\}$ ;
11 end
12  $s \leftarrow \arg \max_{s \in S} \{\text{size}(s)\}$ ;
13 return  $\text{get\_model\_position}(s)$ ;
```

---

The RANSAC calculation algorithm is presented in Algorithm 1. The algorithm has all the signal strength measurements and corresponding positions as input and has the estimated position of the subject as output. A consensus set consists of a number of signal strength readings. Any consensus set uniquely fits a signal strength distribution model within a given error range,  $\gamma$ .  $S$  is a set of candidate consensus sets, which is initialized to be  $\emptyset$  at step 1. Steps 2–10 consist of a loop, which is performed  $f$  times (number of trials). The loop is intended to find  $f$  candidate consensus sets, each of which represents a model. At the beginning of the loop (at step 3), a random set,  $s$ , is initialized with as less data as possible, where,  $b \ll n$ , and  $n$  is the total number of signal strength readings. The set,  $s$ , is enlarged at steps 4–7 with the constraint that the error, how  $s$  fits a model, is less than a predefined error,  $\beta$ . In this way, in each loop, we start from a small random set and find the biggest consensus set within error  $\gamma$ . Finally, at step 11, we can find the biggest consensus set in  $S$ . Then, we can derive a model from this biggest consensus set by the basic MMSE-based calculation (defined in Section 4.2.1).

The function,  $\text{random}(b)$ , randomly selects  $b$  readings and lets them constitute a consensus set. The function,  $\text{error}(s)$ , can be defined as:

$$\text{error}(s) = \min_p \{MSE_p(s)\}.$$

In other words,  $\text{error}(s)$  represents the mean square error of the model which best fits the consensus set,  $s$ . The function,  $\text{get\_model\_position}(s)$ , can be defined as:

$$\text{get\_model\_position}(s) = \arg \min_p \{MSE_p(s)\}.$$

It represents the signal center of the model which best fits the consensus set,  $s$ .



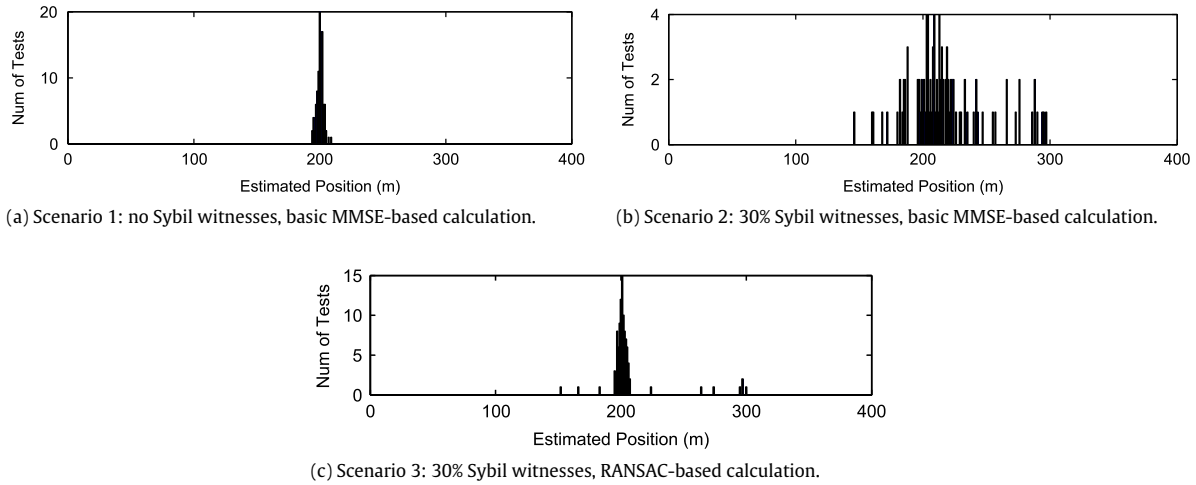


Fig. 2. Estimated position distribution.

We can determine the parameters in this algorithm,  $b, f, \gamma$ , as follows.  $b$  should be as small as possible, and should also be big enough to determine the initial model. Empirically, we set  $b$  to be 4. We suppose that there are  $n$  readings in total,  $m$  of which come from Sybil nodes (we call these readings *fabricated readings*). Therefore, the probability that the initial consensus set does not contain fabricated readings is:

$$P_1 = \frac{\binom{n-m}{b}}{\binom{n}{b}}.$$

Then, the probability that there is at least one consensus set which does not contain fabricated readings in  $f$  trails is:

$$P_2 = \frac{\binom{n-m}{b}}{\binom{n}{b}} f \approx 1.$$

We hope that the initial consensus set is not affected by fabricated readings, so this probability is expected to be 1. Then, we obtain that:

$$f = \frac{\binom{n}{b}}{\binom{n-m}{b}}.$$

This is the number of trials (loops) we should perform in the algorithm, and  $m$  can be regarded as a predefined system parameter, which indicates the level of robustness of the algorithm. It is easy to find that there is a necessary condition,  $m < n/2$ , for our RANSAC-based algorithm. This is because if more than 50% readings are fabricated by Sybil nodes, we must have a consensus set, consisting of only fabricated readings, bigger than any other consensus set. Therefore, 50% is the security resilience threshold for our RANSAC-based approach. The parameter,  $\gamma$ , is exactly the mean square error of the random variable,  $X_{dB}$  (defined in the radio model in Eq. (1)).

Compared to curve fitting (or smoothing), which uses as much input data as possible, RANSAC uses as less data as possible to set up an initial consensus set. Then, this consensus set is enlarged at later iteration steps. Because the method starts from a small consensus set and enlarges it gradually, most of the outlier data will be kept outside of the consensus set. In this way, the algorithm robustness can be improved.

#### 4.3. Simulation

**Scenario I.** In this scenario, we suppose that the signal range is 200 m, the physical position of a claimer is at the point of 200 m,

and all 10 witnesses distributed at random positions faithfully report the measured signal strength from the claimer. In this scenario, we adopt the basic MMSE-based calculation in estimating the claimer's position. Our simulation runs independently for 100 times with different random witness positions, and the distribution of estimated position is shown in Fig. 2(a). From the figure, we can find that the estimated positions of most tests are within 10 m of the real position of the claimer, thereby suggesting that a possible value of threshold  $\theta$  is 10 m. For example, if the distance difference is larger than 10 m, we believe that the claimer is a Sybil node.

**Scenario II.** The basic configurations of Scenario II is the same as Scenario I. However, we assume that the claimer is a malicious node, which claims that its position is at the point of 300 m instead of its real position at 200 m. What is more, 30% of the witnesses are Sybil vehicles. In this scenario, we still use the basic MMSE-based calculation. In order to change the computed result to match the fabricated position (at 300 m), these Sybil witnesses would report fictitious measurements instead of the really measured ones. The results in Fig. 2(b) show that many of the estimated positions have deviated from the real position (at 200 m), moving closer to the fabricated position (at 300 m).

**Scenario III.** Scenario III has the same configurations as Scenario II except that we adopt the RANSAC-based calculation instead of the basic MMSE-based. It is visible in Fig. 2(c) that most of the estimations are close to the real position of the claimer, whereas sporadic points are deviated far away. By analyzing the simulation data, we find that because witnesses are distributed at random positions, it is possible that fabricated readings together with trustworthy readings may happen to constitute a consensus set, which is the reason that fails the RANSAC-based estimation.

**Conclusion.** Based on the above simulation results, we can reach two conclusions. (1) The signal-strength-based verification accuracy is acceptable, given that all witnesses report the real measured signal strength. (2) However, when some witnesses are not trustable, likely selected from Sybil vehicles, the estimated position is not trustable either. The cooperative detection method becomes non-cooperative and cannot detect a Sybil node from its claim. Our RANSAC-based calculation can effectively improve the robustness in estimating the claimer's position. However, it still cannot guarantee an accurate result and also suffers from the 50% security resilience threshold.

**Challenges.** Two challenges still exist. (1) To make the cooperative method effective, we must guarantee that there is no Sybil witness during the detection process. Otherwise, the estimated position may be easily deviated, even we may use the RANSAC-based

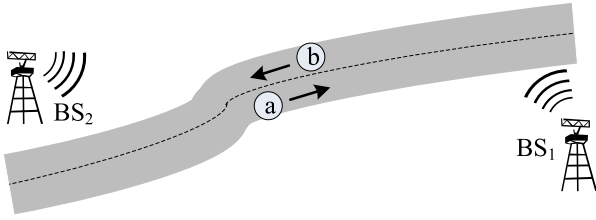


Fig. 3. A scenario with roadside base stations.

calculation to reduce the impact of Sybil witnesses. (2) Threshold (a maximal allowable distance to the claimed position) is not a good rule to judge the Sybil attack. A high threshold may decrease the detection rate (the rate that a Sybil node is detected), but a low threshold may increase the false positive rate (the rate that a normal node is innocently regarded as a Sybil node), which is also not desired. Due to the unstable nature of signal strength measurement, it is difficult to choose an optimal threshold value to meet both the expectations of a high detection rate and a low false positive rate. The following two sections are targeted in these two challenges.

## 5. Presence evidence system

The challenges seem to be a paradox problem. The correctness of our cooperative detection method relies on trusty witnesses. This requires us to know in advance which nodes can be trusted (not Sybil nodes), which is exactly the goal of our method.

Our solution is inspired by the fact that most roads have two-way traffic. We can divide nodes into two groups, each consisting of nodes (vehicles) in the same direction. Then, the previous problem can be changed into: instead of knowing which exact node can be trusted, we only need to know which group of nodes can be trusted. In this way, we can use one trusty group to test the individual nodes in the other group.

In this section, we propose a Presence Evidence System for the purpose of removing Sybil witness candidates. This system is designed to prove when and where a node (vehicle) comes from, and we use this system as a tool to filter witness candidates in a manner that only physical vehicles can remain as witnesses.

As we assumed in Section 3.2, roadside base stations, manipulated by governments, are sparsely distributed along the roads. Then, based on this assumption, we establish the following two rules:

**Rule 1.** A roadside base station would issue a position certification for each vehicle passing by. The position certification contains a time stamp, the passing vehicle's identity, and the location of the base station. Later, it can prove the presence of the vehicle near the base station at a certain time.

**Rule 2.** All witnesses for a claimer should consist of vehicles in the opposite traffic flow to the claimer.

With Rule 1, we can ensure where a certain vehicle comes from. We take Fig. 3 as an example. When node *a* passes by *BS*<sub>2</sub>, it gets a position certificate from base station *BS*<sub>2</sub>, and node *b* also gets one from *BS*<sub>1</sub>. When *a* and *b* meet each other, it is easy for them to prove that they come from the opposite directions by exchanging certificates. When node *a* or *b* broadcasts its position certificates, it signs the broadcasting with a GPS time stamp using its private key. In this way, certificates cannot be rebroadcast by an adversary vehicle.

With Rule 2, we can ensure that each witness in the opposite traffic flow is a physical vehicle instead of a Sybil one. The example in Fig. 1 can illustrate how this rule works. Malicious node *m* fabricates 7 Sybil nodes, in which, *s*<sub>7</sub> is traveling in the opposite direction and the rest the same. When trying to verify the positions

of *s*<sub>1</sub>, . . . , *s*<sub>6</sub>, we only choose witnesses in the opposite (right-to-left) traffic flow such as node *n*<sub>2</sub>, . . . , *n*<sub>5</sub>. However, with Rule 2, we would ignore node *s*<sub>7</sub>, because it cannot prove that it comes from the upstream of the road, and actually it does not. In this way, we can ensure that each witness is a physical vehicle coming from the opposite direction.

With Rules 1 and 2 together, we achieve the goal that the membership of witnesses consists of only physical vehicles, excluding any Sybil vehicle. A verifier would not select witness nodes from the same traffic flow, because it is difficult to judge which witnesses in the same traffic flow are Sybil witnesses. With the help of roadside base stations, the impact of dishonest Sybil nodes on position verification can be effectively removed. Thus, the cooperative method can be applied to detect the Sybil attack accurately.

The Presence Evidence System has the capability to answer and prove questions, such as, where and when have you been? It has a wide variety of potential applications. For example, police can find witnesses for a traffic accident; a car rental company may limit its rental cars in a certain range. We believe more efforts are expected to make this system effective and reliable. In this paper, we take advantage of Presence Evidence System to ensure only physical vehicles are selected as witnesses, but our main focus will be still on exploring the feasibility of using signal strength analysis to detect Sybil nodes.

## 6. Statistical detection method

In this section, we propose a statistical detection method to detect whether a node honestly claims its position. Our method extends observation time to collect more signal strength readings and then perform statistical analysis based on these collected data.

The motivation of our method is inspired by the radio propagation model. From Eq. (1), we can find that the varying of signal strength readings is mainly determined by the noise, *X*<sub>db</sub>, which is supposed to be a Gaussian random variable. In this way, we think we can collect signal strength readings for a period of time and have a test about whether the noise in the readings follows a Gaussian distribution. In other words, if a malicious node fabricates its position, the signal strength measurements cannot match the radio propagation model. We can also extend the observation time to accumulate more measurements.

### 6.1. Basic idea

The basic idea of this method can be described as follows. We let *p* denote the physical position of a node, and *p'* the claimed position. Given a position, we can determine the signal strength distribution model (according to Eq. (2)). Here, we let *m* represent the signal strength model centered at position *p*, and *m'* the model centered at claimed (potentially-fabricated) position *p'*. What is more, *r*<sub>*t,i*</sub> indicates the signal strength measurement at time *t* measured by neighboring vehicle *i*. In this way,

$$e'_{t,i} = r_{t,i} - \text{RSSI}_{p'}(i)$$

represents the measurement noise at position *i* based on model *m'*, and

$$e_{t,i} = r_{t,i} - \text{RSSI}_p(i)$$

represents the measurement noise at position *i* based on model *m*. According to our radio model, sample *e*<sub>*t,i*</sub> should follow Gaussian distribution *X*<sub>db</sub>, and *e'*<sub>*t,i*</sub> should also follow Gaussian distribution *X*<sub>db</sub> if claimed position *p'* matches physical position *p*. In this way, we can obtain a sample set after a period of observation, {*e'*<sub>*t,i*</sub> | *t* ∈ **T**, *i* ∈ **V**}, where **T** is the set of observation times, and **V** is the set of neighboring vehicles at time *t*.

Fig. 4 is a good example to explain our method. In this example, the fabricated position,  $p'$ , is deviated from the physical position,  $p$ . We can find that all the measurements closely follow model  $m$ , which is bound with physical position  $p$ . However, if we use deviated model  $m'$  to calculate the noise  $e'_2$ , we will get a big error, that is,  $e'_2 > e_2$ . This error makes noise samples not follow a Gaussian distribution. Further, this error will become more obvious if we use statistical analysis after accumulating enough samples.

Since the samples used for statistical analysis are determined only by the distance between the physical position and the measurement position, our method can handle signal strength readings from various positions, such as readings from vehicles on a curved road.

The next step is to test whether sample set  $\{e'_{t,i} | t \in \mathbf{T}, i \in \mathbf{V}\}$  follows Gaussian distribution  $X_{dB}$ .

### 6.2. Sample distribution test

In this subsection, we use hypothesis tests to test whether sample set  $\{e'_{t,i}\}$  follows Gaussian distribution  $X_{dB}$ .

Noise sample  $e'_{t,i}$  is supposed to follow the Gaussian distribution  $X_{dB}$  with mean  $\mu = 0$  and variance  $\sigma_{dB}^2$ , where  $\sigma_{dB}$  is the standard deviation of the channel model. Thus the problem is to perform the following two hypothesis tests for the samples,  $\{e'_{t,i}\}$ :

$$\begin{aligned} H_0: \mu_d = 0 & \quad H_1: \mu_d \neq 0 \\ H'_0: \sigma^2 \leq \sigma_{dB}^2 & \quad H'_1: \sigma^2 > \sigma_{dB}^2. \end{aligned}$$

The first test,  $H_0/H_1$ , is to test whether the samples have mean  $\mu = 0$ , and the second test,  $H'_0/H'_1$ , is to test whether the samples have variance  $\sigma_{dB}^2$ .

When both  $H_0$  and  $H'_0$  are true, the method returns that the node honestly claims its position. Since the mean and variance are supposed to be 0 and  $\sigma_{dB}^2$  respectively, the test statistic is

$$|z| = \left| \frac{\bar{e}' - 0}{\sigma_{dB}/\sqrt{n}} \right|,$$

where  $\bar{e}'$  is the mean of sample set  $\{e'_{t,i}\}$ . If  $|z| \geq z_{\alpha/2}$ ,  $H_0$  is rejected; otherwise,  $H_0$  is accepted.  $z_{\alpha/2}$  is the critical value of normal distribution  $N(0, 1)$ , given significance  $\alpha$ .  $\alpha$  is the significance level, a predefined parameter, denoting:

$$P\{\text{Reject } H_0 | H_0 \text{ is true}\} \leq \alpha.$$

Actually,  $\alpha$  also indicates the confidence level of the test result.

Then we use  $\chi$ -test to test the variance  $\sigma^2$ . The test statistic is

$$\chi^2 = \frac{(n-1)s^2}{\sigma_{dB}^2},$$

where  $s^2$  is the variance of sample set  $\{e'_{t,i}\}$ . If  $\chi^2 \leq \chi_{\alpha}^2(n-1)$ ,  $H'_0$  is accepted; otherwise,  $H'_0$  is rejected.  $\chi_{\alpha}^2(n-1)$  is the critical value of  $\chi^2$  distribution, given significance  $\alpha$  and freedom  $(n-1)$ .

In the above test, we are interested in whether there is a significant difference between real physical radio model  $m$  and deviated radio model  $m'$ . Actually, the samples  $\{e'_{t,i}\}$  imply the physical model  $m$ . However, if we use these samples to match the deviated model  $m'$ , it must cause great errors.

One thing, which remains undefined, is the variance,  $\sigma_{dB}$ , of Gaussian distribution  $X_{dB}$ .  $\sigma_{dB}$  indicates the fluctuating range of normal noises. Physically, it means the noise level of the current environment, also implying the realtime channel conditions. It has

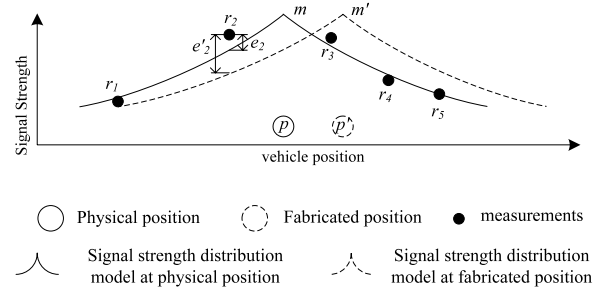


Fig. 4. Noise and distribution model.

a major impact on the hypothesis test results. In the next section, we will discuss how to determine  $\sigma_{dB}$ .

### 6.3. Noise estimation algorithm

A naive method is to set an empirical constant value to  $\sigma_{dB}$ . We can conduct a field experiment, calculate the variance from the signal strength measurements, and use this variance in other environments. The drawback of this naive method is also obvious that a constant variance cannot represent the varying realtime channel conditions.

In this subsection, we use time series forecasting to estimate the current noise level according to the recent noise level history. It works as follows. By the cooperative detection method (in Section 4.1), each node (claimer) periodically broadcasts a beacon. After the beacon interval, the node can accumulate signal strength measurements concerning its previous beacon from its neighbors (witnesses). In this way, the node can obtain a set of noise samples:

$$\{e_{t,i} | e_{t,i} = r_{t,i} - \text{RSSI}_p(i), i \in \mathbf{V}\},$$

where  $t$  represents the time of the previous beacon,  $p$  represents the physical GPS position of the current node, and  $V$  represents the set of the neighbors (witnesses). The node, then, can calculate a variance,  $\sigma_t^2$ , based on this noise sample set. As time elapses, the node can accumulate a time series of variances:

$$\{\sigma_t^2, \sigma_{t-1}^2, \sigma_{t-2}^2, \dots\}.$$

Next, we use exponential smoothing to estimate the noise variance at time  $t+1$ . We set different weights to variance in the history, the more recent with a bigger weight. Then, the estimated variance is:

$$\hat{\sigma}_{t+1}^2 = \sum_{i=0}^{\infty} w_i \sigma_{t-i}^2, \quad (4)$$

where  $\sum w_i = 1$ . Typically, the weight can be defined as:

$$w_i = \beta(1 - \beta)^i,$$

where  $\beta$  is the learning rate, which determines the impact of the most recent variance on the estimated value. Then, Eq. (4) can be written in an iterative way:

$$\hat{\sigma}_{t+1}^2 = \beta \sigma_t^2 + (1 - \beta) \hat{\sigma}_{t-1}^2.$$

The initial value of variance  $\hat{\sigma}_t^2$ , at the very beginning, can be set to an empirical value. However, the node will shortly learn a proper value from the environment.

In this way, each node on roads can periodically update its estimation of the noise variance. This estimation, then, can be used as variance  $\sigma_{dB}^2$  in the hypothesis test (in Section 6.2).





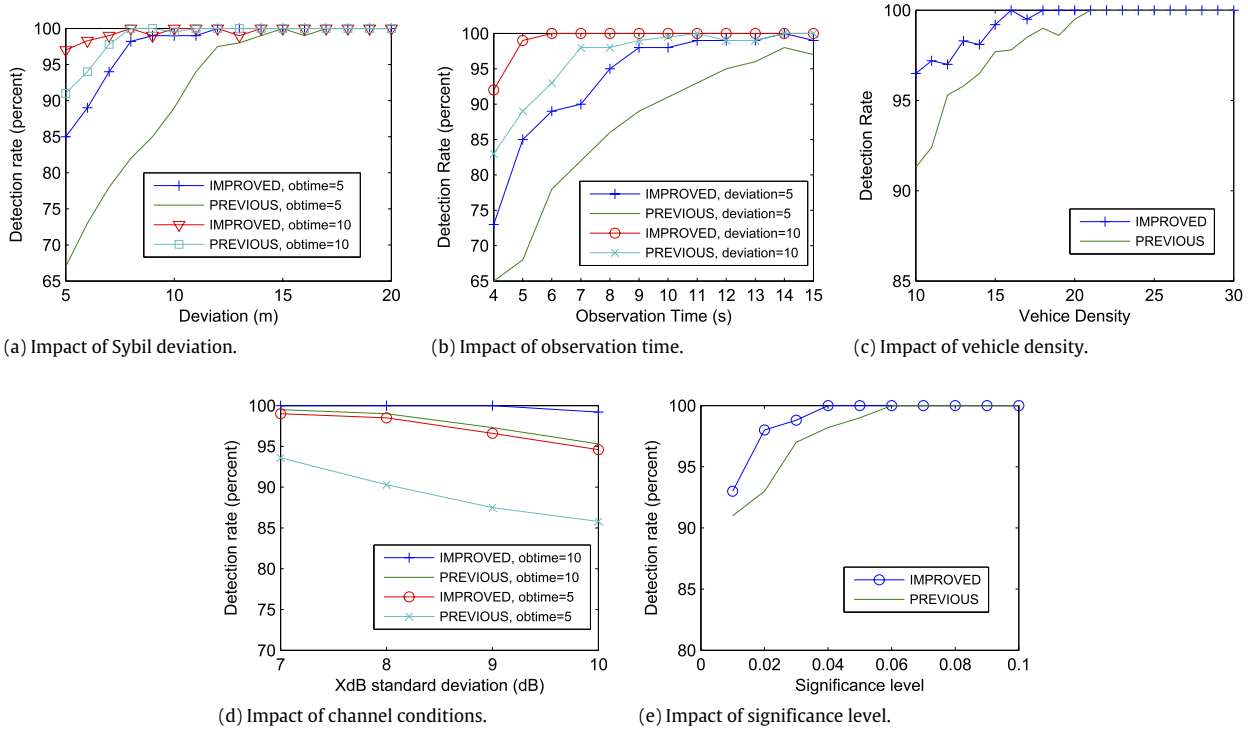


Fig. 5. Detection rate.

In Fig. 5(c), we fix the observation time and the Sybil deviation to their default values, and then we vary vehicle density and record the changes in detection rate. We find that the vehicle density has a major impact on the detection rate. When the vehicle density is large than 20 vehicles per km, both schemes have high detection rates. However, the detection rate of the PREVIOUS scheme drops faster, as the density decreases.

Fig. 5(d) shows the relation between detection rate and  $X_{dB}$  standard deviation. The standard deviation is a parameter which decides the channel stability. In our simulation, we apply the Log-Distance Path Loss Model. Measurements from field tests [16] suggest that signal attenuation can be well modeled using the Log-Distance Loss Model with standard deviation of 9.43 dB in their test environments. The authors suggest that the usual standard deviation in outdoor environment varies from 7 to 9 dB. In our simulation, we vary the standard deviation from 7 to 10 dB. The results show that generally the detection rate decreases with an increase in standard deviation. However, given 10 s of observation time, the IMPROVED scheme can always keep a pretty high detection rate. Fig. 5(e) indicates that the detection rate can also be increased by increasing the significance level. An increase in significance level can increase the critical values of  $z_{\alpha/2}$  and  $\chi^2_{\alpha}(n-1)$  and accordingly increase the probability that  $H_0$  and  $H'_0$  are rejected. However, an increased significant level may also incur an increase in false positive rate. Therefore, a proper value of significant level is a tradeoff between detection rate and false positive rate.

### 8.3. False positive rate

In this subsection, we investigate the impact of system parameters on false positive rate. False positive rate is also an important metric, which represents the possibility that our scheme makes false alarms when there is no Sybil node.

Fig. 6(a) shows the changes in false positive rate as we increase the observation time. Increased observation time allows us to accumulate more signal strength readings and leads to a decrease in false positive rate. Because our IMPROVED scheme has more signal

strength samples for hypothesis tests, it shows better performance in false positive rate than the PREVIOUS scheme. Fig. 6(b) shows the relation between vehicle density and false positive rate. When the vehicle density is low, for the PREVIOUS scheme, it is inaccurate to calculate the estimated position of a target vehicle. Therefore, this inaccuracy may incur a higher false positive rate. Fig. 6(c) shows the impact of channel conditions on false positive rate. From the figure, we can find that even when the standard deviation varies from 7 to 10 dB, our IMPROVED scheme with 10 s observation time can keep the false positive rate at a pretty low level. Fig. 6(d) shows the impact of significance level on false positive rate. If we relate Figs. 6(d) to 5(e), we can find that an increase in significance level may lead to an increase in detection rate, and it also may lead to an increase in false positive rate. Therefore, it is important to find a proper value of significance level to meet the expectation of detection rate and false positive rate. In our simulation, we find that 0.05 would be a proper value of significance level.

## 9. Discussion

In this section, we first present the attack analysis, then discuss several problems related to base stations and opposite traffic, and finally summarize several features of our scheme.

### 9.1. Attack analysis

In this subsection, we are interested in the potential strategies the adversary may apply to crack our detection methods. Since our detection scheme is based on independent and distributed signal strength measurements, in order to make the fabricated Sybil node seem to be close to the claimed position, the malicious node has to deliberately affect the measurement of signal strength. There are two possible ways to impact the signal strength measurements: spoof transmission power and witness penetration. The former attempts to impact the final estimated position from the signal source aspect, while the latter from the witness aspect. We will show that both of these attempts are in vain.

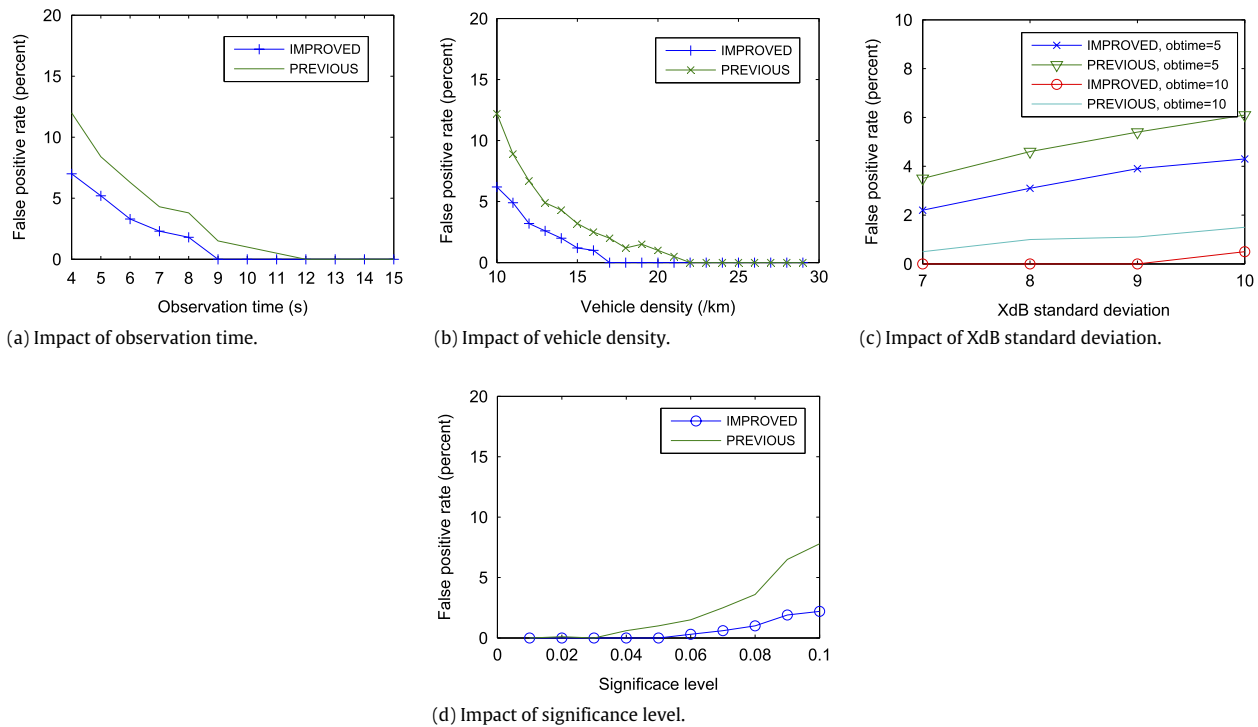


Fig. 6. False positive rate.

In spoof transmission power, Sybil nodes may deliberately decrease or increase the transmission power for broadcasting a beacon message in order to impact the signal strength measurements. However, this attempt is destined to fail, because the change of transmission power will only further deviate the measurements from the supposed signal strength distribution model.

In witness penetration, Sybil nodes, which play the role of witnesses, would cover up for each other and report fabricated signal strength readings. However, we may disable this attempt by using the technique proposed in Section 5. With this technique, all witnesses are selected from the opposite traffic flow, and further they can prove to have come from the upstream of the road, whereas Sybil nodes cannot.

## 9.2. Base stations and opposite traffic flow

In this subsection, we would like to discuss several problems about base stations and opposite traffic flow, which are two important elements for our detection scheme.

In our scheme, roadside base stations do not directly participate in the detection. First, the main responsibility of base stations is to serve as an authority which can prove where a given vehicle comes from. Base stations do not make a judgment about whether a node is a Sybil node or not. Second, base stations are sparsely deployed along roads, and part of road sections might not be covered in the signal range of base stations. Therefore, evidently, base stations cannot detect potential Sybil nodes on those road sections. However, if a road section happens to be covered by a base station, of course, the base station can also serve as a trusted witness for measuring signal strength.

In our methods, we rely on opposite traffic flow to detect Sybil nodes in the current traffic flow. That is because we can identify real physical vehicles in the opposite traffic flow by the technique proposed in Section 5, whereas it is difficult to directly identify real physical vehicles in the current traffic flow (that is our final goal). These physical vehicles in the opposite traffic flow serve as reliable

witnesses for measuring signal strength. However, in case of one-way roads (or two-way but no traffic in the opposite direction), our methods will be incapable of detecting Sybil nodes. We will try to solve this issue in our future work.

## 9.3. Features of our methods

Our detection methods present three unique features. First, our detection scheme can effectively suppress Sybil attacks. Due to the limited accuracy of signal strength-based measurement, we still cannot identify a Sybil node if the claimed position of the Sybil node is very close to the physical position. However, because each vehicle is supposed to occupy a considerable amount of physical space, the greedy vehicle can only fabricated a quite limited amount of vehicles without being detected. Therefore, the Sybil threats can be effectively suppressed. Second, our detection scheme does not rely on specific positioning hardware. Also, even when a malicious node is equipped with multiple radio modules, we still can detect potential attacks, which cannot be achieved by radio resource testing [17]. Finally, our detection scheme is robust and reliable in the sense that it is impossible to change the signal strength distribution pattern from any kind of radio module. As long as reliable signal strength measurements can be guaranteed, the scheme can detect most Sybil attacks.

## 10. Conclusion

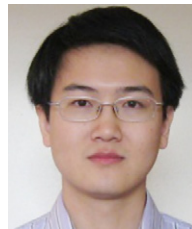
In this paper, we make various attempts to explore the feasibility of using signal strength analysis to detect Sybil attacks. First, we propose a cooperative method to estimate the physical position of a suspicious node. We analyze the constraints of this basic method and further propose two solutions against existing challenges, that is, the Presence Evidence System and the statistical detection method. These approaches can effectively suppress the attacks launched by greedy drivers. Simulations based on real US maps and traffic models prove the performance of our scheme. Although our scheme still cannot guarantee 100% detection, it could

be an economical way to detect Sybil attacks without specific positioning hardware support.

Extensive work is still required in the future. First, our detection scheme requires the support from several sub-systems, such as, the Presence Evidence System and the channel noise estimation. We only introduced the basic ideas of these sub-system and more efforts are expected. Second, since signal strength readings are not accurate in nature, if Sybil nodes are claimed to be very close to the physical vehicle, it is hard to distinguish the Sybil nodes. We may resort to a geometric model to define the minimal distance between two vehicles.

## References

- [1] P. Bahl, V.N. Padmanabhan, RADAR: an in building rf-based user location and tracking system, in: Proc. of IEEE Infocom 2000, pp. 775–784, 2000.
- [2] J.J. Blum, A. Eskandarian, L.J. Hoffman, Challenges of intervehicle ad hoc networks, IEEE Transactions on Intelligent Transportation Systems 5 (4) (2004) 347–351.
- [3] S. Brands, D. Chaum, Distance-bounding protocols, in: Proc. of Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, Springer-Verlag, Inc., 1994, pp. 344–359.
- [4] S. Capkun, J.-P. Hubaux, Secure positioning of wireless devices with application to sensor networks, in: Proc. of Infocom 2005, pp. 1917–1928, 2005.
- [5] M. Demirbas, Y. Song, An RSSI-based scheme for Sybil attack detection in wireless sensor networks, in: Proc. of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks, 2006.
- [6] 5.9 GHz DSRC, <http://grouper.ieee.org/groups/scc32/dsrc/index.html>.
- [7] M.A. Fischler, R.C. Bolles, Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography, Communications of the ACM 24 (6) (1981) 381–395.
- [8] M. Ghosh, A. Varghese, A. Gupta, A. Kherani, Detecting misbehaviors in VANET with integrated root-cause analysis, Ad Hoc Networks 8 (7) (2010) 778–790.
- [9] P. Colle, D. Greene, J. Staddon, Detecting and correcting malicious data in VANETs, in: Proc. of ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2004, pp. 29–37, 2004.
- [10] GrooveNet, <http://www.andrew.cmu.edu/user/rahulm/Research/GrooveNet/>.
- [11] D. Hadaller, S. Keshav, T. Brecht, S. Agarwal, Vehicular opportunistic communication under the microscope, in: Proceedings of ACM MobiSys'07, pp. 206–219, 2007.
- [12] J.P. Hubaux, S. Capkun, J. Luo, The security and privacy of smart vehicles, IEEE Security and Privacy Magazine 2 (3) (2004) 49–55.
- [13] G. Korkmaz, E. Ekici, Urban multi-hop broadcast protocol for inter-vehicle communication systems, in: Proc. of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2004, pp. 76–85, 2004.
- [14] T. Leinmuller, C. Maiher, E. Schoch, F. Kargl, Improved security in geographic ad hoc routing through autonomous position verification, in: Proc. of ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2006, pp. 57–66, 2006.
- [15] R. Mangharam, D.S. Weller, D.D. Stancil, R. Rajkumar, J.S. Parikh, GrooveSim: a topography-accurate simulator for geographic routing in vehicular networks, in: Proceedings of Second ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2005, Cologne, Germany, 2005.
- [16] J.J. Meyers, Channel characterization and reliability of 5.8 GHz DSRC wireless communication links in vehicular ad hoc networks in suburban driving environment, Master Thesis, Carnegie Mellon University, 2005.
- [17] J. Newsome, E. Shi, D. Song, A. Perrig, The Sybil attack in sensor networks: analysis & defenses, in: Proc. of the Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, pp. 259–268, 2004.
- [18] NS2, Network Simulator. <http://www.isi.edu/nsnam/ns/>.
- [19] S. Park, B. Aslam, D. Turgut, C.C. Zou, Defense against Sybil attack in vehicular ad hoc network based on roadside unit support, in: Proc. of Military Communications Conference, 2009.
- [20] B. Parno, A. Perrig, Challenges in securing vehicular networks, in: Proc. of the Fourth Workshop on Hot Topics in Networks, HotNets-IV, 2005.
- [21] T.S. Rappaport, Wireless Communications, Principles and Practice, Prentice Hall, 1996.
- [22] M. Raya, J.-P. Hubaux, The security of vehicular networks, in: Proc. of the 3rd ACM Workshop on Security of ad Hoc and Sensor Networks, SASN 2005, pp. 11–21, 2005.
- [23] M. Raya, J.P. Hubaux, Securing vehicular ad hoc networks, Journal of Computer Security 15 (1) (2007) 39–68. (Special Issue on Security of Ad Hoc and Sensor Networks).
- [24] N. Sastry, U. Shankar, D. Wagner, Secure verification of location claims, in: Proc. of the 2003 ACM Workshop on Wireless Security, WiSe 2003, pp. 1–10, 2003.
- [25] M. Torrent-Moreno, H. Hartenstein, P. Santi, Fair sharing of bandwidth in VANETs, in: Proc. of ACM Workshop on Vehicular Ad Hoc Networks, VANET 2005, pp. 49–58, 2005.
- [26] B. Xiao, B. Yu, C. Gao, Detection and localization of Sybil nodes in VANETs, in: Proc. of the 2006 Workshop on Dependability Issues in Wireless ad Hoc Networks and Sensor Networks, 2006.
- [27] R.M. Yadumurthy, A. Chimalakonda, M. Sadashivaiah, R. Mankanaboyina, Reliable mac broadcast protocol in directional and omni-directional transmissions for vehicular ad hoc networks, in: Proc. of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2005, pp. 10–19, 2005.
- [28] G. Yan, S. Olariu, M.C. Weigle, Providing VANET security through active position detection, Computer Communications 31 (12) (2008).
- [29] J. Zhao, G. Cao, VADD: vehicle-assisted data delivery in vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 57 (3) (2008).



**Bo Yu** received his Ph.D. degree in Computer Science in 2007 from Fudan University, China. He was a Post-doc Fellow in the Department of Electrical and Computer Engineering, Wayne State University, USA. His research interests include wireless sensor networks, mobile ad hoc Networks, and vehicular networks, with a focus on information dissemination and resource management.



member of the IEEE.

**Cheng-Zhong Xu** received his Ph.D. degree in Computer Science from the University of Hong Kong in 1993. He is currently a Professor in the Department of Electrical and Computer Engineering of Wayne State University, and the Director of the Cloud and Internet Computing Laboratory (CIC) and Sun's Center of Excellence in Open Source Computing and Applications (OSCA). His research interest is mainly in scalable distributed and parallel systems and wireless embedded computing devices. He has published two books and more than 160 articles in peer-reviewed journals and conferences in these areas. He is a senior



**Bin Xiao** received the B.Sc. and M.Sc. degrees in electronics engineering from Fudan University, China, in 1997 and 2000, respectively, and the Ph.D. degree in computer science from the University of Texas at Dallas in 2003. After his Ph.D. graduation, he joined the Hong Kong Polytechnic University as an assistant professor. Currently, he is an associate professor in the Department of Computing at the Hong Kong Polytechnic University, Hong Kong. His research interests include mobile cloud computing, data management, network security, wireless sensor networks, and RFID systems. He is an associate editor for the International Journal of Parallel, Emergent and Distributed Systems. Dr. Xiao is a recipient of the Best Paper Award from IEEE/IFIP EUC 2011. He is a senior member of the IEEE.