This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

Multi-channel based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI

Yuan Yao, *Member, IEEE,* Bin Xiao, *Senior Member, IEEE,* Gaofei Wu,
Xue Liu, *Member, IEEE,* Zhiwen Yu *Senior Member, IEEE,* Kailong Zhang, *Member, IEEE,* and Xingshe Zhou, *Member, IEEE*

Abstract—Vehicular Ad Hoc Networks (VANETs) bring many benefits and conveniences to road safety and drive comfort in future transportation systems. However, VANETs suffer from almost all security issues as same as wireless networks. Sybil attack is one of the most risky threats since it violates the fundamental assumption of VANETs-based applications that all received information are correct and trusted. Sybil attacker can generate multiple fake identities to disseminate false messages. In this paper, we propose a novel Sybil attack detection method based on Received Signal Strength Indicator (RSSI), Voiceprint, to conduct a widely applicable, lightweight and full-distributed detection for VANETs. Unlike most of previous RSSI-based methods that compute the absolute position or relative distance according to RSSI values, or make statistic testing based on RSSI distributions, Voiceprint adopts RSSI time series as the vehicular speech and compares the similarity among all received series. Voiceprint does not rely on any predefined radio propagation model, and conducts independent detection without support of the centralized node. Moreover, we improve Voiceprint by allowing it to conduct detection on Service Channel (SCH) to shorten observation time. Furthermore, we extend Voiceprint with change-points detection to identify those illegitimate nodes performing power control. Extensive simulations and real-world experiments demonstrate that Voiceprint is an effective method considering the cost, complexity and performance.

Index Terms—Sybil attack, vehicular ad hoc networks, received signal strength indicator, multi-channel, dynamic time warping

1 Introduction

Vehicular Ad Hoc Networks (VANETs) is a promising technology to address the challenging issues in the intelligent transportation system (ITS) such as accident avoidance, traffic monitoring and transport efficiency. VANET enables a vehicle to directly communicate with neighboring vehicles (vehicle-to-vehicle, V2V) as well as roadside infrastructures (vehicle-to-infrastructure, V2I). VANETs can provide a wide range of communication-based vehicle safety and non-safety applications in ITS such as intersection collision avoidance, cooperative collision warning, blind spot warning, emergency electronic brake lights, lane change assistance, traffic flow control and enhanced route guidance and navigation.

Dedicated Short Range Communications (DSRC) at 5.9 GHz is a set of protocols for VANETs issued by the Federal Communications Commission (FCC) in 1999. There are two kinds of communication devices defined in DSRC, namely the On Board Unit (OBU), which is installed in the vehicle, and the Road Side Unit (RSU), which is deployed on the roadside. Safety-related messages are broadcasted periodically on the Control Channel (CCH) by OBUs with the kinematic information. Meanwhile, non-safety messages could be sent on the Sevice Channel (SCH) to provide some non-safety applications such as navigation and infotainment.

The main purpose of VANETs is to improve the road safety as well as raise the traffic efficiency. Nevertheless, VANETs inherit all security vulnerabilities from the wireless networks, which becomes the major issue to apply this technology into practice. Many types of attacks can be launched in VANETs, but one of harmful is Sybil attack [1]. As aforementioned, many safety or non-safety applications in VANETs such as cooperative collision warning and enhanced navigation need cooperation of other vehicles. This requires one vehicle gets enough credible information from legitimate vehicles. However, in Sybil attack, adversary generates multiple fake identities to create many untrusted virtual nodes in VANETs. It violates the fundamental assumption in implementing those applications [2].

In Sybil attack, the attacker is usually called malicious node and the simulated virtual nodes are called Sybil nodes. For instance, a malicious vehicle may fabricate a large number of virtual vehicles with fake identities and false locations. This makes an illusion of a heavy traffic ahead for other vehicles nearby. Then, the neighboring vehicles may choose other routes while the attacker can get the good road condition. Moreover, Sybil attacker can do even more harm to VANETs by launching further attack. The malicious node may flood target vehicles or RSUs via multiple Sybil nodes with useless messages to reduce the network performance. It is the well known DoS attack. In the other case, the malicious node may make seemingly disjoint paths in multipath routing protocol in fact all converge to it via multiple Sybil nodes. Then, the malicious node could drop all the messages go through it and launch black hole attack.

Due to the severe damage when Sybil attack happens,

Yuan Yao, Gaofei Wu, Zhiwen Yu, Kailong Zhang and Xingshe Zhou are with Northwestern Polytechnical University, Xian, 710072, China(E-mail:yaoyuan,gfwu,zhiwenyu,kl.zhang,zhouxs@nwpu.edu.cn).
Bin Xiao is with The Hong Kong Polytechnic University, Hong Kong(E-mail: csbxiao@.comp.polyu.edu.hk).
Xue Liu are with the McGill University, Montreal, Quebec, Canada(E-mail: xueliu@cs.mcgill.ca).
Manuscript received XX XXX. XXXX; revised XX XXX. XXXX; accepted XX XXX. XXXX. Date of publication XX XXX. XXXX; date of current version XX XXX. XXXX.
(Corresponding author: Xiao Bin.)
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier no. XX.XXXX/TMC.XXXX.XXXXXXX

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

many detection methods are proposed by researchers. All these techniques can be classified into three categories: resource testing based, trusted certification based and position verification based mechanisms. The resource testing based methods may become invalid if the malicious node has more computation or communication resources, and they bring extra overhead to the system. Most of the trusted certification based methods run the detection algorithms in a centralized manner which are not suitable for the VANETs due to the fast changing dynamic topology. In addition, the deployment of public key infrastructure and the high complexity of cryptographic algorithms are also uncertain issues in this type of methods. Considering the low cost, wide availability and decentralized nature, the RSSI-based position verification methods are better for detecting Sybil attacks in the initial stage of VANETs.

In this paper, we proposed a novel Sybil attack detection method, Voiceprint to conduct a widely applicable, lightweight and full-distributed detection for VANETs. Unlike most of previous RSSI-based methods that compute the absolute position or relative distance according to the average RSSI values, or make statistic testing based on RSSI distributions, Voiceprint compares the RSSI time series as the vehicular speech. This approach is based on the major observation in our real-world experiments that the RSSI time series of Sybil nodes have the very similar patterns. The main contribution of this paper is five-fold:

1) The proposed method does not rely on any radio propagation model which can be widely applied to different road environments (model-free, widely applicable);
2) Each single node as a detector can make independent detection without any help of other vehicles, thus, it does not require to establish the credibility of neighboring nodes (trust relationship-free, lightweight);
3) We implement a full-distributed algorithm without any centralized control or support of RSU (infrastructure-free, full-distributed).
4) We allow Voiceprint to conduct detection on SCH which greatly shorten the observation time and reduce the false positive rate.
5) We leverage Bernaola Galvn Segmentation Algorithm (BGSA) [3] to detect abrupt changes in RSSI time series in order to identify those illegitimate nodes performing power control.

The rest of this paper is organized as follows. Section 2 reviews the related work. Section 3 reveals several important observations from the field tests that motivate our work. Section 4 presents our proposed detection method in detail. Section 5 conducts simulations to evaluate our approach. Section 6 carries out further experiments in a real DSRC testbed. Finally, Section 7 draws the conclusion.

2 Related Work

Sybil attack is a very critical problem in distributed peer-to-peer systems. It was first introduced by Douceur [4] in the distributed storage system. Extensive works are done to detect the malicious node and Sybil nodes in these systems. The goal of these detection methods is to ensure each physical node is bound with a valid unique identity [5]. All these methods can be classified into three categories: resource testing based, trusted certification based and physical measurement based mechanisms.

2.1 Resource Testing Based Methods

This type of approaches assumes that each physical node has limited resources such as computation, storage and communication resources. If a malicious node fabricates many Sybil nodes, it cannot pass the corresponding testing simultaneously.

Douceur in [4] used computational puzzles to test computation resource for each identity. The detector generates a large number of random puzzles to challenge each node simultaneously. If a node cannot find the result within a limited time, it is probably a Sybil node. Thus, this approach is in vain if the malicious node is equipped with sufficient computation resources. Newsome et al. proposed another resource testing method that adopts communication channels to test each node [6]. They indicated that Sybil nodes cannot transmit messages on different channels at the same time. So they let the detector assigns different channels to neighboring nodes to broadcast, and it then selects a random channel to listen. If the detector does not hear any message on that channel, the assigned identity is a Sybil node. Because the channel is randomly chosen, the detector will find all Sybil nodes with multiple test rounds. Therefore, this approach is not suitable for a difficult case that there are too many nodes with insufficient channels. In that case, the number of test rounds increases exponentially. Moreover, channel testing brings extra overhead in communications which may lead to channel congestion.

2.2 Trusted Certification Based Methods

Trusted certification based methods are the most popular techniques to establish trust relationship among all nodes. This type of approaches usually uses the certificate authority, public key infrastructure, digital signatures and cryptographic algorithms to ensure the trustworthiness of each identity.

Raya et al. designed the Vehicular Public Key Infrastructure (VPKI) framework for VANETs [7]. It details key management, authentication and key revocation mechanisms. However, the VPKI deployment is still an uncertain issue that needs heavy and complex efforts to do. Park et al. proposed an economical solution suitable for the initial stage of VANETs [2]. They used timestamp series issued by RSU to detect Sybil nodes. The major assumption of this approach is that two different vehicles rarely pass through a few same RSUs at the same time. Each message should include at least the last two timestamps, and these timestamp series between two Sybil nodes are always very close. This method requires extra hardware namely Tamper-Proof Device (TPD) installed in each vehicle to guarantee the timestamp authorized by RSU cannot be modified. Moreover, it is hardly applied to complex urban environment since malicious node who collects enough timestamps can create legal series by choosing a subset of the timestamps. Chen et al. proposed a similar approach called RobSAD

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

to detect Sybil nodes by comparing the difference between two trajectories (timestamp vectors broadcasted by RSU) [8]. This method is also suitable for the early stage of VANETs because of limited requirements of RSU. However, it still does not solve the remained problem in [2]. Chang et al. proposed a scheme named Footprint to detect Sybil attack to solve above problem [9]. When a vehicle approaches to the range of a RSU, it demands a authorized message containing RSU's identity and the timestamp to verify the vehicle presents in a certain RSU's vicinity at the particular time. Then, each vehicle can generate a trajectory with all the messages it records along the road. A node who wants to detect the Sybil nodes around will first exclude the distinct trajectories using check window and trajectory length limit, because the probability of two vehicles having exactly the same trajectories is slim. Then, the left ones may have some fabricated trajectories with the subset of timestamps. They transferred this detection problem into finding all complete subgraghs in an undirected graph. This approach solves the above issues but it needs each vehicle to know the whole layout of RSUs' deployment in order to establish the undirected graph. In addition, the complexity of pair wise trajectory comparison and finding Sybil nodes is very high. Zhou et al. proposed a privacy preserved solution P2DAP [10]. In this scheme, they assumed the department of motor vehicle (DMV) is the trusted entity which maintains a pseudonyms pool and manages pseudonyms for all vehicles. To avoid abuse of multiple pseudonyms by one malicious vehicle, P2DAP distributes several pseudonyms with the same hash value to one vehicle. If a RSU hears one event sent by two pseudonyms with same hash value, it reports suspected vehicles to DMV to make final judgment. Since RSU is seen as semi-trusted party that might be compromised, the authors adopted two level hash functions with different keys (coarse-grained keys and fine-grained keys). RSU only keeps the coarse-grained keys which does not know whether the pseudonyms belong to one vehicle or not, while DMV stores all keys and can detect Sybil nodes by two level hashing. This approach detects Sybil attack meanwhile preserves privacy of vehicles. However, DMV will become a bottleneck in the large, heavy network traffic because of excessive communication in the network. To overcome this drawback, Mekliche et al. [11] improved P2DAP. In their work, RSUs perform additional role in the system to distinguish Sybil nodes from suspected identities. If two suspected vehicles are verified in the similar position, RSU determinates them as Sybil nodes. Alimohammadi et al. proposed a Boneh-Shacham (BS) short group signature based scheme for solving two conflicting goals privacy and Sybil attack in VANETs [12]. Reddy et al. proposed a cryptographic digital signature based method to establish the trust relationship between participating entities [13].

Trusted certification based methods can find Sybil nodes at the beginning of the attack. However, this type of approaches usually requires a centralized trust party to issue digital signatures or certificates which cannot easily applied in the initial stage of VANETs. In addition, due to the fast changing dynamic topology of VANETs and the high complexity of cryptographic algorithms, the lightweight and decentralized detection method is more suitable for the vehicular environment.

2.3 Position Verification Based Methods

Position verification based methods usually adopt some physical measurements such as Received Signal Strength Indicator (RSSI), Angle of Arrival (AoA) and Time Difference of Arrival (TDoA) to detect Sybil attack. These measured values only depend on the hardware and physical environment that cannot be easily forged or modified by the malicious node.

RSSI-based techniques are low-cost methods without any specialized hardware. It is on the basis of the idea that receiver can estimate distance from the sender according to RSSI values using theoretical radio propagation models. Then, with multiple neighboring nodes' information, a detector is able to get the position of a certain node by solving the equations. Demirbas et al. used RSSI-based localization method to detect Sybil nodes in a static Wireless Sensor Network (WSN) [14]. They adopted ratio of RSSIs from multiple receivers to overcome the time varying and unreliable nature of measured RSSI values. Extensive indoor experiments proved that even two cooperative detector nodes are sufficient to detect a Sybil node. Lv et al. proposed a Cooperative RSSI-based Sybil Detection (CRSD) scheme [15]. CRSD does not compute accurate positions, but distances among different nodes. Then, each node groups the identities with similar RSSI together and broadcasts this suspect group result to other nodes. Finally, each node takes the largest intersection among all received groups as the detected Sybil nodes. All above RSSI-based methods are decentralized techniques without the centralized infrastructure. However, these methods detect Sybil attack in a cooperative manner that each node needs the help of neighboring nodes, i.e., to get RSSI values observed by other nodes around to solve the equations or compute the intersection of suspect groups. Therefore, the major problem in these methods is how to confirm the credibility and honesty of the neighboring nodes, since the Sybil nodes fabricated by the malicious node might send forged RSSI values to impede the detection.

To avoid this problem, Bouassida et al. proposed an independent detection method based on RSSI [16]. In this scheme, the authors checked RSSI variations measured successively if they fall into a reasonable interval or not. The unreasonable nodes are labeled as "suspect". Then, distinguishability degrees are evaluated by estimating the geographical localizations of each suspect node. Identities with the similar estimated locations are considered as Sybil nodes. This method can be launched individually by every node without sharing RSSI values. But the authors only verify the proposed methods in a small scale testbed. The maximum distance between two nodes is 10m in experiments. Chen et al. proposed a centralized approach based on RSSI [17]. In this scheme, landmark as the trusted centralized party records all RSSI values transmitted by sensors and conducts a statistical testing for each two RSSI distributions. The nodes have similar RSSI distributions are Sybil nodes. Chen's work was designed for static WSNs, Shrestha applied this method into VANETs which simply removed the landmark from the network and compared RSSI distributions in each single node [18]. Xiao and Yu [19][20] proposed a cooperative detection method considering the trust relationship among all neighboring nodes.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

In this cooperative detection method, each vehicle performs the role of claimer, witness, and verifier. As a claimer, one vehicle periodically broadcasts its identity and position. The verifier will collect the claimers information plus its RSSI series from neighboring nodes within an observation time. Then, each node as a verifier estimates the position of the claimer by using the received RSSI series and the predefined propagation model. If the claimed position fails to match the estimated position, it is judged as Sybil nodes. To avoid some Sybil nodes provide forged location information, they assumed each vehicle can receive a position certification when passing through an RSU. And the witnesses only selected from the opposite traffic flow which has the issued position certification. According to this certification, this cooperative method can ensure that each node in witness group is a trusted physical entity. The proposed method overcomes the major issue of establishing trust relationship in the cooperative detection algorithms. However, it is not suitable for the dense traffic and one-way roads. Garip proposed INTERLOC that used other mobile nodes to localize a vehicle [21]. INTERLOC continuously learned changing interference levels by using an interference-aware radio propagation model. Then, it adjusted the interference level accordingly so as to improve the localization accuracy.

RSSI-based techniques are lightweight compared to trusted certification based methods, and usually performed in the decentralized manner. These features make it more suitable for the VANETs with the fast changing dynamic topology.

Some unresolved major issues of RSSI-based Sybil attack detection methods in VANETs are summarized as below:

1) All these RSSI-based methods assume certain propagation models to estimate positions of neighboring nodes. The estimation accuracy heavily depends on the chosen model. Although some experimental results proved that they might work well in the static WSN or low mobility MANET, they are unfeasible for high mobility VANETs, since the rapid changing of the network topology, irregularity of the wireless medium and the complexity of the road environment (effects of reflection, refraction, diffraction, multi-path and shadowing produced by buildings, trees and other obstacles) make the predefined radio propagation model inaccurate.
2) Most of RSSI-based methods are decentralized but cooperative detection that require exchanging information among neighboring nodes. Therefore, each node as a detector should know the credibility of every node sharing the information around it and ensure all received messages are trusted and correct. The common approach is either to establish trust relationship among all neighboring nodes or to design a full-distributed algorithm of independent detection.
3) Some RSSI-based methods use centralized detections that need a trusted central base station to perform detection operations. And some ones establish the trust relationship in support of the RSU. The nationwide deployment of such infrastructures is hard to achieve at the initial stage of VANETs. Even in the mid-term stage, there might be still many places uncovered by RSU.
4) All previous RSSI-based methods have a serious security vulnerability that they cannot identify illegitimate nodes manipulating transmission power deliberately during Sybil attacks.

3 Measurements and Observations

As most of RSSI-based methods heavily rely on the assumed radio propagation models, we should first assess the effectiveness of such models in the real vehicular environment. In this Section, we conduct several real-world experiments using multiple vehicles equipped with DSRC radios in different scenarios.

3.1 Measurement Equipments

The experiment includes four vehicles that each one is equipped with an IEEE 802.11p compliant radio, namely the IWCU OBU4.2 produced by ITRI. The onboard equipments for each vehicle are composed of an IWCU OBU4.2 unit, a 5.9GHz antenna, a GPS module and a laptop which are shown in Figure 1.

Fig. 1: Measurement equipments

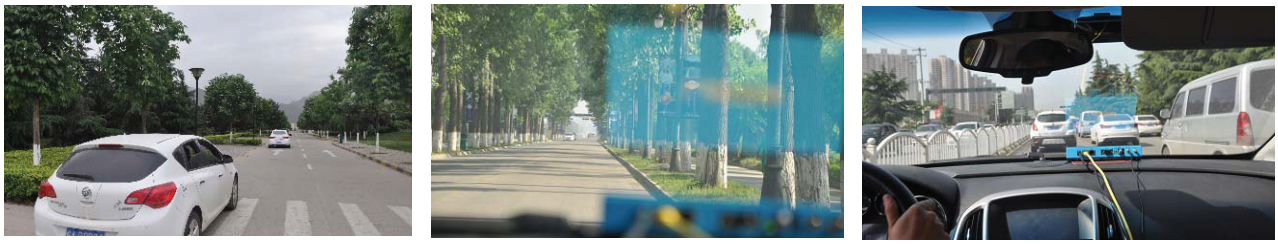
IWCU OBU4.2 is a WAVE/DSRC communication device mounted in a vehicle. It is embedded Linux machine (kernel 2.6.32) based on a 32 bits MIPS processor (Atheros AR7130) working at 300MHz. It has two Ethernet interfaces, a GPS connector and a DSRC radio based on the standard IEEE 802.11p-2010 [22]. It provides 5 discrete power levels: 15, 17, 20, 23 and 25 dBm. IWCU OBU4.2 is connected to the 5.9GHz omni-directional antenna with a gain of 7dBi. The antenna is mounted on the roof of the vehicle. There is also a rooftop GPS receiver placed by the side of the antenna to log the vehicle's position. The IWCU OBU4.2 also connects to the laptop via an Ethernet interface, thus, the laptop can record the RSSI value of each successfully received packet. The details of equipments are listed in Table 1.

3.2 Measurement Scenarios

To assess the effectiveness of RSSI-based position verification methods in VANETs, we conduct several experiments in different scenarios. Each vehicle adopts WAVE Short Message Protocol (WSMP) provided by IWCU OBU4.2 SDK software toolkit to send single-hop broadcast with its identity, GPS coordinates, direction and velocity. At receiver, the connected laptop records all received RSSI values via Ethernet.

Scenario 1: This measurement is carried out in the campus of Northwestern Polytechnical University, Xi'an.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

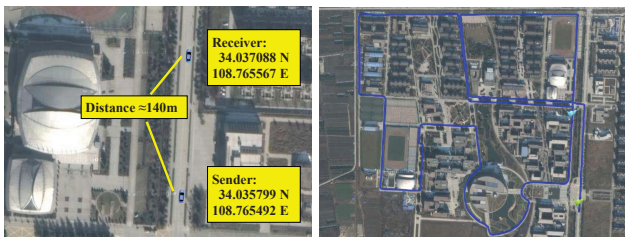


(a) Campus (b) Rural area (c) Urban area

Fig. 3: Scenario 2 (snapshots of different environments)

TABLE 1: Details of measurement equipments

Equipment	Details
Processor	Atheros AR7130 300MHz (MIPS 32bit)
DSRC radio	IEEE 802.11p, RX sensitivity: -95 dBm
Antenna	5.9GHz, 7dBi Omni
GPS module	50 channels, A-GPS support, sensitivity: -160 dBm, accuracy of time-pulse signal: 30ns (RMS), horizontal position accuracy: <2.5m (autonomous), <2.0m (SBAS)
Ethernet	10/100 Mbps (RJ45) port, full-duplex
Power level	15, 17, 20, 23, 25dBm
Channel width	10MHz/20MHz
Standards compliance	IEEE 802.11p-2010, IEEE 1609.2-v2-d9 3-2011-09, IEEE 1609.3-2010, IEEE 1609.4-2010



(a) Stationary (b) Mobility

Fig. 2: Scenario 1 (Two vehicles communicate in the campus)

The scenario is shown in Figure 2a. Two vehicles keep stationary with each other at a distance about 140m. The sender broadcasts its information 10 packets per second, and the receiver records RSSI values from the sender. We conduct this experiment two times at different time period, each one lasts 10mins. Another measurement is also carried out in the campus, but vehicles move around the schoolyard as shown in Figure 2b. The speed of vehicle approximately is 10-15 km/h.

Scenario 2: In this case, we collect data from different areas including campus, rural area and urban area to illustrate the impact of the environment to the propagation models. Figure 3 gives snapshots of different areas.

Scenario 3: In this scenario, we simulate the Sybil attack with four vehicles as shown in Figure 4. There are three normal nodes (marked in blue) and one malicious node (marked in yellow) with motion at the same direction. The malicious node generates two fake identities i.e. Sybil nodes (marked in red) at false locations. During the experiment, the normal node 1 and 3 are ahead of and behind the malicious node respectively. The normal node 2 keeps moving with the malicious node side by side. The normal node 1 and 3 record all RSSI values from the malicious node, the fabricated Sybil nodes 1 and 2 and the normal node 2.

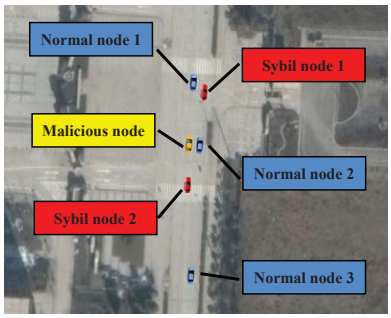


Fig. 4: Scenario 3 (four vehicles simulate Sybil attack)

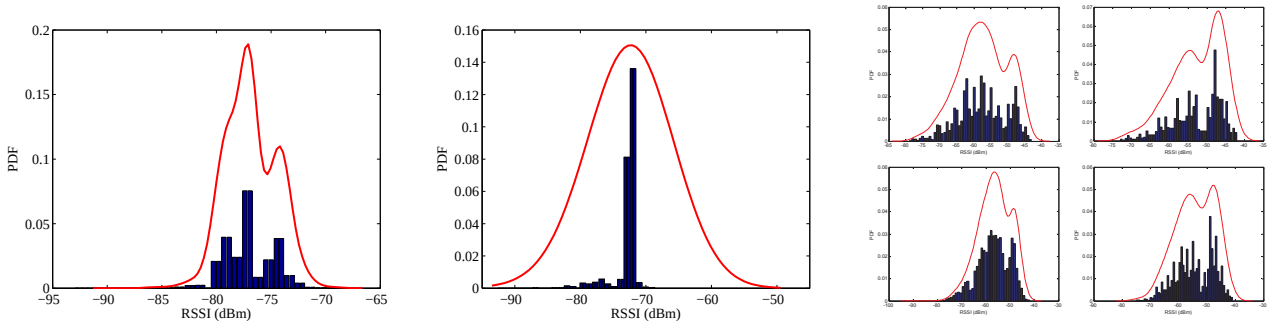
Scenario 4: This scenario is almost the same as ***Scenario 3***. The only different setting is that we allow malicious node to change power arbitrarily for itself and the fabricated Sybil nodes.

3.3 Observations

We plot the RSSI distributions of Scenario 1 in Figure 5. Figure 5a and 5b show the RSSI values recorded when two vehicles keep stationary in two different periods. Each distribution contains 6000 samples. The mean and square deviation of two distributions are (-76.8600 dBm, 2.3266 dBm) and (-72.5390 dBm, 0.7654 dBm) respectively. According to free space path loss model and two-ray ground propagation model assumed in [14] and [15], the average distances between two vehicles are estimated to be 281.5m (free space path loss model in the first period) and 171.2m (free space path loss model in the second period), 263.9m (two-ray ground propagation model in the first period) and 205.8m (two-ray ground propagation model in the second period), respectively. Comparing to the ground truth 140m, the estimated values are quite inaccurate.

Figure 5c give four RSSI distributions of different segments randomly selected from Scenario 1 that two vehicles move around the campus. Each segment has 1 mins long, thus, contains 600 RSSI samples. In some RSSI-based position verification methods [19, 21, 22], they assume the RSSI series follow the normal distribution according to the shadowing model. Actually, the RSSI values barely show the normal distribution in VANETs, especially when the vehicle keeps moving constantly.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing



(a) 2016/05/09 14:31:50 - 14:41:50 (stationary)(b) 2016/05/09 15:06:14 - 15:16:14 (stationary)(c) Four segments selected randomly (mobility)

Fig. 5: RSSI distributions

From the results obtained in Scenario 1, we get the first observation.

Observation 1: **The channel quality changes over time in VANETs (Temporal variation). Therefore, a predefined propagation model might lead to significant errors in position estimation or make false statistic testing based on the wrong assumption of RSSI distribution.**

We establish a dual-slope piecewise linear model [23] based on empirical measurements , as shown in Eq. 1, is used to approximate the path loss using linear regression on the measured data sets.

$$P_r(d) = \begin{cases} P(d_o) - 10\gamma_1 log_{10}\left(d/d_o\right) + X_{\sigma 1}, d_0 \leq d \leq d_c \\ P(d_o) - 10\gamma_1 log_{10}\left(d_c/d_o\right) - 10\gamma_2 log_{10}\left(d/d_c\right) \\ +X_{\sigma 2}, d > d_c \end{cases} \tag{1}$$

Due to the sparsely distributed vehicles in campus and rural area, there is a dominant Line-Of-Sight (LOS) path between receiver and sender. The breakpoint distances (dc) are much longer than the value in the urban area since more densely distributed obstacles like vehicles and pedestrians on the road cause severe signal distortion at receivers in Non Line-Of-Sight (NLOS) conditions. In addition, the signal attenuation in the campus environment seems much better than the rural area because the effects of reflection and shadowing are probably more serious by those high and dense wayside trees (shown in Figure 3a and 3b).

Then, we have the second observation.

Observation 2: **The channel conditions are not the same in different areas considering complex reflection, refraction, diffraction and multi-path effects caused by buildings, trees and other obstacles (Spatial variation). For a predefined propagation model, it requires to set different parameters for different environments. However, it is very hard for a vehicle to sense the environment dynamically, and then to determine optimal parameters.**

Figure 6 gives the measured RSSI time series by the normal node 1 and 3. Then, we have a significant and interesting observation.

Observation 3: **The RSSI time series of the malicious node and the Sybil nodes have very similar patterns. The series of the malicious node and the normal node 2 are similar, but still have some differences even if they always keep very close distance (2.75-3.25m) during the motion.**

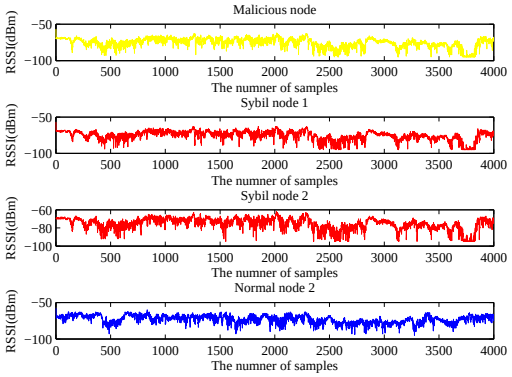


Fig. 6: RSSI time series of malicious node, Sybil nodes and normal node

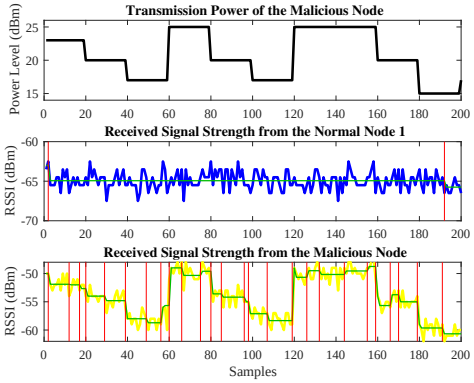


Fig. 7: RSSI time series of malicious node with power control

Figure 7 shows the measured RSSI time series from the malicious node and normal node 1. In this scenario, the malicious node change its transmission power randomly, thus, the normal node cannot detect the Sybil attack according to similarity comparison. However, we find another important phenomenon when analyzing these series by BGSA.

Observation 4: **RSSI time series received from illegitimate nodes who manipulate the transmission power during the Sybil attack within an SCH interval (50ms) show a lot of abrupt changes in mean. Since the displacement**

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

between two vehicles is only $0.25 \sim 3m$ during an SCH interval, the RSSI variations due to vehicle mobility could be neglected. Therefore, the frequent changes in RSSI time series imply that the transmitter conducts power control.

With above observations, we extend the Voiceprint method with a multiple change-points detection method, i.e. Bernaola Galvn Segmentation Algorithm (BGSA) [3], to identify those malicious nodes who manipulate their transmission power deliberately.

4 Sybil Attack Detection using Vehicular Voiceprint

In this section, we first describe the attack model and assumptions. Then, we introduce the similarity measures for time series. Finally, we give the detailed Sybil attack detection algorithm based on vehicular voiceprint.

4.1 Attack Model and Assumptions

In this paper, we focus on the simultaneous Sybil attack that each Sybil attacker concurrently creates multiple fake identities to disrupt normal functionalities of VANETs. Figure 8 shows a typical Sybil attack scenario in the highway environment. From this figure, the legitimate vehicle bounded with unique valid identity is referring to the normal node (marked in blue). The physical vehicle uses multiple forged identities is called malicious node (marked in yellow), and the claimed virtual identities are Sybil nodes (marked in red).

Assumption 1: We assume there may be several Sybil attackers in VANETs, but those malicious nodes do not collude to use other attackers' identities. The attacker only creates new identities rather than stealing other vehicle's identity. In other words, there is no same identity existed simultaneously in the network.

Assumption 2: In VANETs, every vehicle is equipped with only one DSRC radio and one 5.9GHz antenna. The radio operates in the CCH/SCH alternating switch mode. It broadcasts safety messages on CCH 10pkts/sec and is forced to send test messages on SCH 100pkts/sec.

Assumption 3: The normal nodes may have different initial TX_powers since we assume heterogeneous onboard devices, but they do not conduct power control during communications. The malicious node may change TX_Power for itself and the fabricated Sybil nodes arbitrarily.

Assumption 4: We assume a very early stage of VANETs that there is no RSU or other base station deployed on the road for vehicle to infrastructure communications.

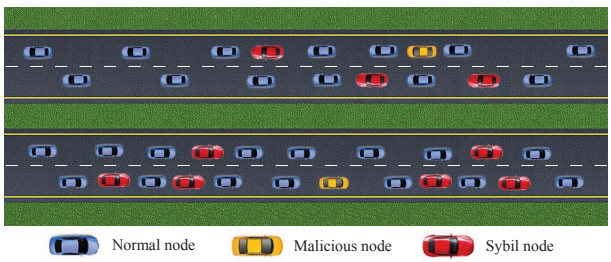


Fig. 8: An example of Sybil attack scenario in VANETs

4.2 Similarity Measures for Time Series

Time series is a sequence of data points successively collected over time. With the ***Observation 3*** obtained from the real-world experiments, we find that the RSSI time series of Sybil nodes have very similar patterns. Therefore, we detect Sybil attack by measuring the similarity between two RSSI time series based on this important observation. Here, similarity is an absolute value computed by comparing or matching the resemblances between two series. Commonly, a distance function D(X,Y) is defined to represent the similarity between time series X and Y.

Since time series similarity measures have been a major topic in data mining research for decades, many distance functions have been proposed in this domain. The classical form to compute the similarity is Lp norm. When p equals to 2, it is the well-known Euclidean distance.

Another commonly used distance is called Dynamic Time Warping (DTW). DTW adopts dynamic programming technique to determine the best matching between two time series by warping the series in the temporal domain. Given two time series with different length N and M, $X_N(x_1, x_2, ...x_i, ...x_N)$ and $Y_M(y_1, y_2, ...y_j, ...y_M)$, DTW first establishes an N-by-M cost matrix C containing distance $c_{i,j}$ between each pair of points x_i and y_j. The cost $c_{i,j}$ is usually used Euclidean distance as:

$$c_{i,j} = (x_i - y_j)^2 \tag{2}$$

Then, DTW computes the minimum accumulated cost $D_{i,j}$ for each pairwise matching (i, j) between two series recursively by:

$$D_{i,j} = c_{i,j} + \min\{D_{i-1,j}, D_{i,j-1}, D_{i-1,j-1}\} \tag{3}$$

where $D_{0,0}$ is set to be 0 initially and other value in the accumulated cost matrix D are initialized to ∞.

After that, DTW constructs a optimal warp path $W = w_1, w_2, ..w_k, ...w_K$ ($w_k = (i, j)$ means the i^{th} element of X is aligned to the j^{th} element of Y) with the minimum total accumulated cost. The optimal warp path W must start from $w_1 = (1, 1)$ to $w_K = (N, M)$ to ensure all points of both series are matched. In addition, the warp path should also satisfy the monotonicity constraints which is defined as:

$$\begin{aligned} &IF\ w_k = (i, j), w_{k+1} = (i', j');\\ &THEN\ i \le i' \le i + 1, j \le j' \le j + 1 \end{aligned} \tag{4}$$

Finally, the DTW distance is measured as the total accumulated cost:

$$D_{DTW}(X, Y) = D_{N,M} \tag{5}$$

Wang et al. make an extensive comparison for 13 different similarity measures using 38 data sets from various application domains [24]. The main conclusion drawn by the study is that the DTW distance is superior to the other newly proposed methods considering the accuracy in the vast majority of cases, and the well-established Euclidean distance is also a robust, simple, generic and efficient way to measure the similarity of time series. From above introduction of these two distances, we find that the Euclidean distance matches in the point-to-point way, which requires two time series having the same length. DTW distance overcomes this

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

limitation that can tolerate the shifting, scaling and warping of series in the temporal domain, which is widely used in speech recognition to cope with different speeking speeds. Considering that packet loss often occurs in VANETs, we cannot always get two RSSI series with exactly the same length. Therefore, we use DTW distance to measure the similarity of RSSI time series like vehicular voiceprint recognition. However, despite the accuracy of DTW scheme, it has $O(N^2)$ time complexity in general since it should fill all cells in the NM cost matrix. So, we adopt FastDTW [25] in this paper. FastDTW speeds up DTW distance measure by adding constraints and data abstraction to limit the cost cell evaluation. Then, it achieves $O(N)$ time complexity while has only 1% loss of accuracy, which can meet the real-time requirements in Sybil attack detection.

4.3 Change-points Detection for Time Series

According to the ***Observation 4***, we notice that RSSI time series of the malicious node performing power control show lots of abrupt changes in mean. This problem can be defined as dividing the time series into many segments with different mean value, which is to maximize the difference in the mean values between adjacent segments. We adopt BGSA to solve this problem.

To divide a time series $X(x_1, x_2, ...x_N)$ of length N into stationary segments of constant mean, it needs to move a sliding pointer from left to right along the series. At each position j, we compute the mean values of two subseries: μ_{left} for $(x_1, x_2, ..., x_j)$ and μ_{right} for $(x_{j+1}, x_{j+2}, ..., x_N)$.

To measure the difference between both means, we conduct the *t*-test:

$$t = \left| \frac{\mu_{left} - \mu_{right}}{\sqrt{\sigma}} \right| \tag{6}$$

where σ is the pooled variance:

$$\sigma = \frac{N\left(SD_{left} + SD_{right}\right)}{(N-2)\, j\, (N-j)} \tag{7}$$

where SD_{left} and SD_{right} are the standard deviations of two subseries.

Then, it determines the position of the pointer for which the t reaches its maximum value, t_{max}. The significance level $\mathcal{P}(\tau)$ of a possible change-point with $t_{max} = \tau$ is defined as the probability of obtaining the value τ or lower values within a random sequence:

$$P(\tau) = \mathrm{Prob}\{t_{\max} \leq \tau\} \tag{8}$$

Thus, a series of N random numbers of fixed mean would remain unsegmented with probability $\mathcal{P}(\tau)$. If the significance of t_{max} is smaller than a predefined threshold p_0 (significance level), the pointer is decided as a change-point. Then, we continue the method recursively on the newly created subsequences, until none of the possible change-points satisfy $t_{max} \leq p_0$. Finally, we get a segmented series at the significance level p_0.

4.4 Proposed Detection Methodology

In this subsection, we present our Sybil attack detection method, namely Voiceprint, based on similarity measurement and change-points detecion of RSSI time series. Voiceprint does not rely on any predefined radio propagation model, and it also does not require the support of centralized nodes (RSUs or base stations). Each vehicle conducts independent detection locally without establishing trust relationship among neighboring vehicles.

There are three phases in Voiceprint, collection, comparison and confirmation.

4.4.1 Collection

According to ***Assumption 2***, each vehicle mounts a DSRC compliant OBU operating on CCH/SCH alternating switch mode as shown in Fig. 9.

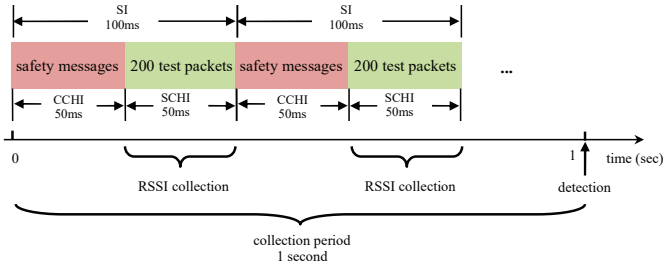


Fig. 9: The CCH/SCH alternating switch mode

In the multi-channel alternating switch mode, a Synchronization Interval (SI) is divided into a CCH Interval (CCHI) and a SCH Interval (SCHI), each of them has 50ms length. In our previous work [26], we collect RSSI values on CCH. Since the safety message frequency is defined as 10HZ in the standard IEEE 802.11p, it needs at least 20 seconds to collect 200 RSSI values from one neighbouring vehicle. To shorten data collection time, we force each OBU to send 200 test packets (the test packet should contain vehicle ID) on SCH during service channel interval (there is no restrictions on messages transmission frequency in SCH), thus, to collect 200 packets from one vehicle just requires 0.1 second. All neighboring nodes could receive test packets and measure the RSSI value for each successfully received packet. In the collection phase, one vehicle monitors the SCH and records all the latest messages within a constant interval (this interval is called observation time in this paper). Actually, for each packet, Voiceprint only needs to store a 2-tuple $< ID, RSSI >$, and then generates RSSI time series for each received IDs. Here, RSSI time series of vehicle i is denoted by $RSSI_i$.

4.4.2 Comparison

After sufficient observation time for collection, we first detect multiple change-points in RSSI time series to identify those illegitimate nodes performing power control. Then, we make comparison between every pair wise RSSI time series. As aforementioned, we use DTW distance to measure the similarity of RSSI time series. However, based on ***Assumption 3***, if the malicious node deliberately increase or decrease the initial TX Power for different Sybil nodes,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

the similarity of RSSI time series among malicious node and Sybil nodes can be simply broken, because the relative distance between each aligned points is enlarged. To solve this problem, we conduct a data preprocessing before the comparison which normalizes every RSSI time series by an enhanced Z-score normalization:

$$RSSI'_i = \frac{RSSI_i - \mu}{3\sigma} \tag{9}$$

where μ and σ are the mean and standard deviation of $RSSI_i$ respectively. This normalization makes 99.7% values fall into the range of (-1, 1). In this normalization, the whole shape and structure of RSSI time series cannot be changed, but the relative distances among Sybil nodes' RSSI series by spoofed transmission power are perfectly eliminated.

After data preprocessing, we compare each two RSSI time series and measure the DTW distance. Then, we conduct a postprocessing for obtained DTW distances to normalize all values into the range of [0, 1] using min-max normalization as follows:

$$D'_{DTWi,j} = \frac{D_{DTWi,j} - D_{DTW\,\min}}{D_{DTW\,\max} - D_{DTW\,\min}} \tag{10}$$

where $D_{DTW\,\min}$ and $D_{DTW\,\max}$ are the minimum and maximum values of all DTW distances respectively.

4.4.3 Confirmation

In comparison process, each vehicle can get a group of series change-points and DTW distances for all neighboring vehicles. Based on ***Observation 3***, DTW distances among all Sybil nodes should be very small that are closer to 0, while DTW distances between Sybil nodes and normal nodes or among all normal nodes should be much bigger. However, from extensive simulations in Section 5, we find that DTW distances are easily distinguishable in the low vehicle density, but have a small overlap when the density increases. There are two reasons for this phenomenon. First, when the traffic gets jammed, the average space between two vehicles is shorten, thus, the RSSI time series of malicious node and some normal nodes nearby are also very similar. Second, with the increasing traffic density, the number of nodes in VANETs is also increased. This leads to severe channel collisions that cause a lot of packet losses in the whole network. Thus, the similarity of RSSI time series among all Sybil nodes is decreased. The overlap will reduce the detection rate and increase the false positive rate when the traffic density increases if we set a constant threshold. To deal with this problem, we just think of the threshold as a function of density. And the determination of the threshold can be transformed into a binary classification problem that finds the optimal decision boundary (actually a line in the two-dimensional condition) in the density-DTW distance plane. There are many methods such as perceptrons algorithm, linear classifier, logistic regression and support vector machines proposed to do classification in machine learning. In this paper, we use the Linear Discriminant Analysis (LDA) to determine the threshold. For an estimated density den and a measured DTW distance $D_{DTWi,j}$ between node i and node j, each vehicle can distinguish the Sybil nodes from normal nodes as following:

$$\begin{aligned} &IF\ D_{DTWi,j} \le k_1 den + b_1; \\ &THEN\ adding\ IDs\ i\&j\ to\ suspect\ group \end{aligned} \tag{11}$$

where k_1 and b_1 is the slope and intercept of the decision boundary. These parameters can be obtained by training based on our simulation or experiment data.

According to ***Observation 4***, we notice that illegitimate nodes conducting power control show a large number of change-points. Similarly, we also adopt LDA to determine the decision boundary with the slope k_2 and intercept b_2.

Each vehicle can estimate traffic density in a simple way as:

$$den = \frac{N_{normal}}{2Dist_{\max}} \tag{12}$$

where N_{normal} is the number of normal nodes it can hear within the density estimation period. $Dist_{max}$ is the maximum distance from these normal nodes (suppose that GPS information can be used to calculate the distance).

Moreover, to decrease the false positive rate, we determine a suspect node as a Sybil node after several detection periods (called determination times denoted by N).

The procedure of Voiceprint is presented in Algorithm 1.

Algorithm 1 Voiceprint

Require:
$RSSI_n$: RSSI time series
ID_n: Corresponding IDs
P_0: Significance level
den: Estimated traffic density
k_1: Slope of DTW distance decision boundary
b_1: Intercept of DTW distance decision boundary
k_2: Slope of change-points decision boundary
b_2: Intercept of chengepoints decision boundary
N: Determination times
Ensure:
$SybilIDs$: Suspect IDs of Sybil nodes

```
SybilIDs = {ALL IDs}
for t = 1 to N do
    for i = 1 to n do
        RSSI_i ← Z-score-normalization(RSSI_i)
        N_CPi ← BGSA(RSSI_i,p0)
        if N_CPi ≤ k2 · den + b2 then
            SuspectIDs_t = AddingIDs(i)
        end if
    end for
    for i = 1 to n − 1 do
        for i = 2 to n do
            if i<j then
                D_DTWi,j ← FastDTW(RSSI_i, RSSI_j)
            end if
        end for
    end for
    D_DTW ← Min-max-normalization(D_DTW)
    for i = 1 to n − 1 do
        for i = 2 to n do
            if i<j then
                if D_DTWi,j ≤ k1 · den + b1 then
                    SuspectIDs_t = AddingIDs(i, j)
                end if
            end if
        end for
    end for
    SybilIDs = SuspectIDs_t ⋂ SybilIDs
end for
return SybilIDs
```

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

5 Simulation Evaluation

In this section, we evaluate the performance of the proposed Voiceprint using NS2 simulations.

5.1 Simulation Setup

We conduct our simulation in the NS-2.34 simulator and use the empirical propagation model given in equation (1) [23]. To prove that Voiceprint does not depend on any predefined propagation model, we set a timer in NS2 and modify the parameters of the propagation model periodically. The simulation scenario is a 2km bi-directional highway with 2 lanes in each direction as shown in Figure 10. Vehicles re-enter the highway at the beginning of the other direction when they arrive at the end of one direction. For an individual simulation run, we randomly set 5% vehicles as malicious nodes, and each one generates 3-6 Sybil nodes. 20% of these illegitimate nodes conduct power control. All nodes broadcast 10 packets per second, but the malicious node should send $10n$ packets if it fabricates n fake identities. The initial transmission power can be randomly selected from 5 power levels for each node, but remains constant during the simulation.

We adopt a continuous-time stochastic mobility model to simulate vehicle motion. In this model, each vehicles movement is divided into a sequence of random time intervals called mobility epochs. The epoch lengths are identically, independently distributed (i.i.d.) exponentially with mean $1/\lambda_e$. During each epoch, the vehicle moves at a constant speed which is an i.i.d. normal distributed random variable with mean μ_v and the standard deviation σ_v. The default parameters are given in Table 2.

TABLE 2: Default parameter settings

Parameter	Value
Highway length	2km
Lanes	4
Lane width	3.6m
Density	10-100 vhls/km
Density estimate period	10s
Vehicle number	20-200
Model change period	30s
μ_1	1.66-2.56
μ_2	5.53-6.34
σ_1	2.8-3.9dB
σ_2	3.2-5.2dB
d_0	1m
d_c	102-218m
Frequency	5.9GHz
Bandwidth	10MHz
Transmission Power	17-23dBm
Date rate	3Mbps
Packet size	500Bytes
Packet generation rate	10Hz
Slot time	13μs
SIFS	32μs
Mobility epoch rate (λ_e)	$0.2s^{-1}$
Average speed (μ_v)	25m/s
Standard deviation of the speed (σ_v)	5m/s
Observation time (detect on CCH)	20s
Detection period (detect on CCH)	1min
Observation time (detect on SCH)	1s
Detection period (detect on SCH)	10s
Significance level (p_0)	0.1
Determination times	6
Simulation time	100s

5.2 Metrics and Threshold

5.2.1 Metrics

We consider two main metrics to evaluate our scheme, i.e., detection rate (DR) and false positive rate (FPR). For a single normal node and one detection period, detection rate is the proportion of detected suspect nodes to the total number of illegitimate nodes within all its neighboring vehicles. False positive rate is the percent of normal nodes are incorrectly detected as forged ones. For a single normal node i, it receives multiple packets from N_i different nodes during the observation time. Assume that in the k^{th} detection period, there are $N_{i,k}^n$ legitimate nodes, $N_{i,k}^m$ malicious nodes and N_j^s Sybil nodes generated by the j^{th} malicious node. If it correctly detects $N_{T,k}$ fabricated nodes and wrongly identifies $N_{F,k}$ normal nodes. Then, the detection rate and false positive rate for node i in the k^{th} detection period are defined as follows:

$$DR_{i,k} = \frac{N_{T,k}}{N_{i,k}^m + \sum_{j=1}^{N_{i,k}^m} N_j^s} \tag{13}$$

$$FPR_{i,k} = \frac{N_{F,k}}{N_{i,k}^n} \tag{14}$$

Assume we have totally N_n normal nodes and each normal node detects K times during the simulation. Then, the average detection rate and average false positive rate can be calculated as follows:

$$\overline{DR} = \frac{1}{N_n K} \sum_{i=1}^{N_n} \sum_{k=1}^{K} DR_{i,k} \tag{15}$$

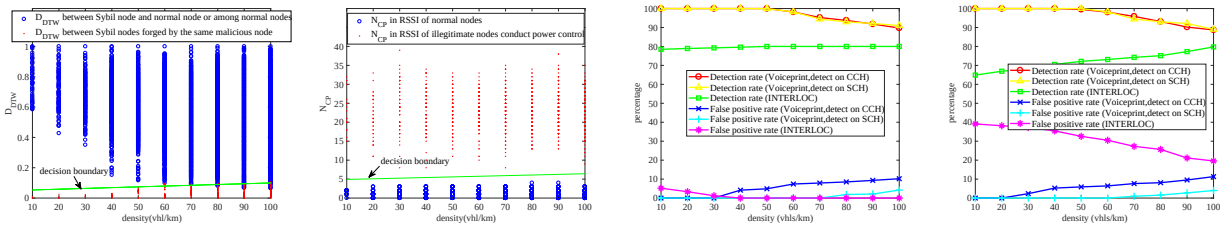
$$\overline{FPR} = \frac{1}{N_n K} \sum_{i=1}^{N_n} \sum_{k=1}^{K} FPR_{i,k} \tag{16}$$

In the simulation, we use the average detection rate and average false positive rate to evaluate the performance of Voiceprint.

5.2.2 Threshold

In this paper, we leverage LDA to find the decision boundary. Each node can tune the threshold according to the estimated traffic density. We first conduct several simulations for different traffic densities (5 simulation runs at each density) and record all measured change-points and DTW distances. Then, we use these features as the training data to compute the optimal decision boundary, i.e. to determine the slope and intercept for the divider line. The results are shown in Figure 10. In Figure 10a, the blue cycle denotes the DTW distance between the Sybil node and the normal node or between two normal nodes. The red dot is the DTW distance between two Sybil nodes forged by the same malicious node. In Figure 10b, the blue cycle is the number of change-points in RSSI of normal nodes, while the red dot is the number of change-points in RSSI of illegitimate nodes. After training, the parameters of k_1, b_1, k_2 and b_2 are set to be 0.00054, 0.0483, 0.0167 and 4.75 respectively.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing



(a) Threshold of DTW distances (b) Threshold of change-points number (c) Without propagation model change (d) With propagation model change

Fig. 10: Thresholds and simulation results

5.3 Results and Analysis

In our simulations, we compare the Voiceprint with the interference-aware RSSI-based localization sybil attack detection scheme (INTERLOC) proposed in [21].

Figure 10c shows the detection rate and false positive rate of two methods without propagation model change. The standard deviation σ_1 and σ_2 are both set to be 3.9dB during the simulation. From Figure 10c, we see that the performance of INTERLOC is improved with the increasing vehicle density, while Voiceprint has the opposite trend. This is because INTERLOC is the cooperative detection method. One vehicle conducts Sybil attack detection which not only uses the RSSI values observed by its own, but also adopts information received from neighboring vehicles. With the increasing traffic density, each vehicle could collect more information from other vehicles nearby. Since Voiceprint is the independent detection scheme, one vehicle only uses RSSI time series observed locally. Therefore, with the increasing traffic density, the severe packet losses lead to less information obtained by each vehicle, thus, reduce the detection rate. Moreover, the dense traffic means the shorter average space among vehicles. Thus, vehicles cannot easily distinguish Sybil nodes from normal nodes nearby that results in the increasing false positive rate.

Figure 10d gives the results with propagation model change. The model parameters are modified periodically during the simulation. We can observe that the performance of INTERLOC drops rapidly, while Voiceprint is almost immune to the change. Although INTERLOC dynamically adjust the interference level, it still uses the predefined model parameters. These parameters can hardly cover all conditions in complicated vehicular environments to get an accurate interference level estimation. Since Voiceprint does not rely on any propagation models, it is widely applicable for different environments and complex conditions.

In both scenarios, Voiceprint can achieve to 90% level detection rate and low false positive rate under 10%. However, INTERLOC can barely identify 20% illegitimate nodes performing power control.

We also compare the improved Voiceprint detected on SCH with the Voiceprint detected on CCH. From figures 10c and 10d, we observe that the Voiceprint detected on SCH has lower false positive rate than the Voiceprint detected on CCH. This is because we final determine Sybil nodes after multiple detections. Any time the node is detected as a normal node, it will be removed from the suspected group.

Figure 11 shows the impact of the number of RSSI samples on the detection rate and computation time (density = $100vhls/km$). From the figure, the detection rate increases with the number of samples. The computation time of Voiceprint is linearly related to the number of samples. Take into consideration of both factors, we collect 200 samples from each neighbouring node.

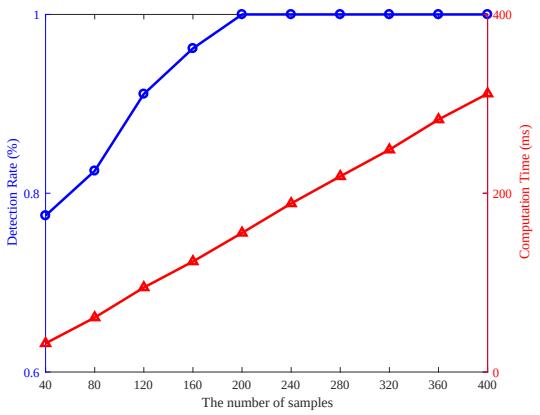


Fig. 11: The impact of samples on performance of Voiceprint

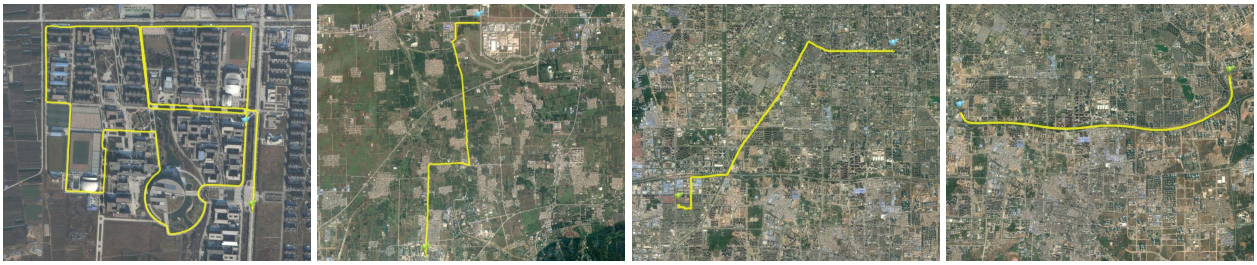
6 Field Test

In this section, we evaluate the performance of the proposed Voiceprint in the real-world field test.

6.1 Experiment Setup

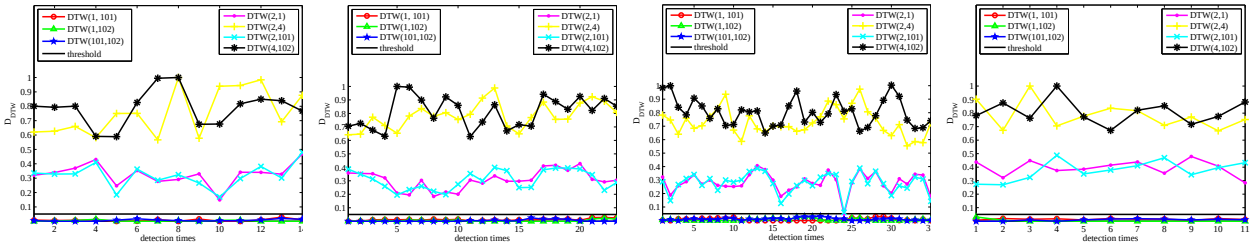
In this field test, we use four vehicles equipped with DSRC radios and embedded with the Voiceprint application. We conduct a series of experiments under campus, rural area, urban area and highway environments shown in Figure 12. There are one malicious node (ID = 1) and three normal nodes (IDs = 2, 3 and 4), and the malicious node generates two Sybil nodes with two fake identities (IDs = 101 and 102). The setup is same to Figure 4 given in Section 3.2 ***Scenario 3***. Normal node 2 moves as close as possible to the malicious node during the test. The initial transmitted powers of all physical nodes (nodes 1-4) are 20dBm. The initial transmitted powers of Sybil node 101 and 102 are 23dBm and 17dBm respectively. We record RSSI time series and conduct detections on CCH and SCH at the same time. The observation time is 20s and 1s, detection period is 1min and 10s on CCH and SCH respectively. Since there are only

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing



(a) Campus (3.5km) (b) Rural area (11.2km) (c) Urban area (15.4km) (d) Highway (12.7km)

Fig. 12: The routes of different areas in field tests



(a) Campus (b) Rural area (c) Urban area (d) Highway

Fig. 13: The DTW distances recorded by normal node 3 on CCH

four vehicles in the network, we just set a constant threshold to be 0.05046 at the traffic density of 4vhls/km.

We are further carrying out more experiments in the urban area at different time periods (non-peak hour at 10:00 and peak hour at 18:00). In these experiments, we allow illegitimate nodes to conduct power control. Specifically, the malicious node changes its transmission power randomly during the Sybil attack, while the normal nodes and fabricated Sybil nodes keep the constant power during communications. According to the trained decision boundary for change-points detection, the threshold is set to be 4.8168.

6.2 Results and Analysis

The durations of tests in different areas are 13min21s, 22min 40s, 34min46s and 11min12s respectively. Thus, detections are totally conducted 14, 23, 35 and 11 times on CCH (detection period is 1min on CCH) in campus, rural area, urban area and highway correspondingly. We store all measured DTW distances and compare them with the threshold. Figure 13 plots the results recorded by normal node 3 on CCH. Here, $DTW(a, b)$ means the measured DTW distance of RSSI time series received from the node a and b.

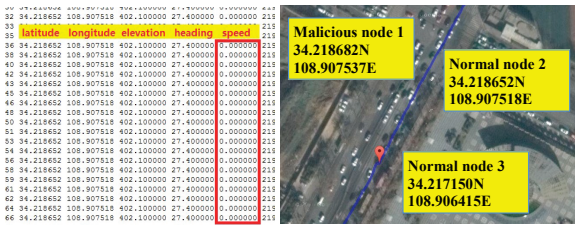


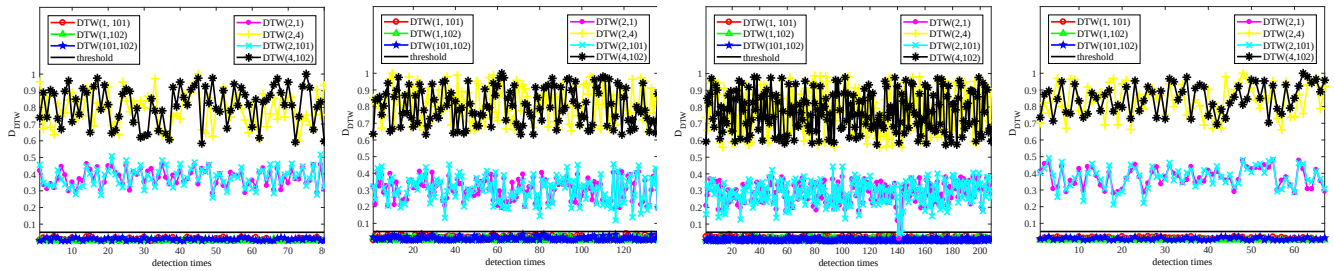
Fig. 14: The location of the false detection

From Figure 13, we can find that the detection rate is 100% in all scenarios and the false positive rate is 0.95%, only one time that the normal node 2 is incorrectly detected as the Sybil node. We further analyze the GPS traces shown in Figure 14. According to GPS traces of malicious node 1, normal node 2 and 3, we notice that all these nodes remain stationary without mobility at this detection. Based on the locations of nodes on the map, we find that the false detection occurs at the intersection. The reasonable explanation is that all vehicles stop at the intersection waiting for a red light. The distances between each pair of nodes are 3.8m (node 1 and 2), 198.9m (node 1 and 3) and 195.2m (node 2 and 3) respectively. Therefore, the normal node 3 cannot distinguish two RSSI time series from malicious node 1 and normal node 2 since all nodes remain stationary in this detection period, which leads to very similar signal patterns between node 1 and 2 (Notice that node 3 is very far away from these two nodes, most of RSSI values are -95dBm which reaches the RX Sensitivity of our radio).

We also record RSSI of test packets and measure DTW distances on SCH at the same time. Since the detection period is 10s on SCH, detections are totally conducted 80, 136, 208, 67 times on SCH. The measured DTW distances by normal node 3 on SCH are shown in 15. Similarly, we find that there are three false detections on SCH in the urban environment. However, Voiceprint detected on SCH does not false alarm since it makes final decision after 6 detection periods. Voiceprint detected on SCH can greatly shorten observation time, thus, enable us to conduct more detections during a small period. The improved Voiceprint outperforms the Voiceprint detected on CCH that achieve 100% detection rate and 0% false positive rate in the field test under all road conditions.

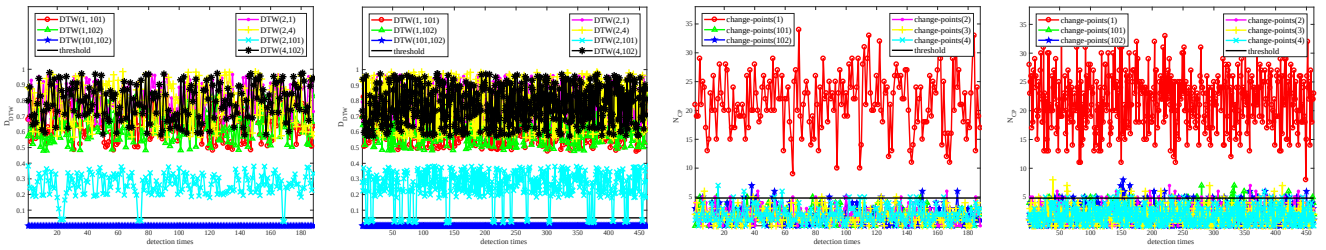
From the real-world experiments, we show that the proposed Voiceprint is suitable for different areas, especially in the rural and highway environments where vehicles can

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing



(a) Campus (b) Rural area (c) Urban area (d) Highway

Fig. 15: The DTW distances recorded by normal node 3 on SCH



(a) D_{DTW} (non-peak hours) (b) D_{DTW} (peak hours) (c) N_{CP} (non-peak hours) (d) N_{CP} (peak hours)

Fig. 16: Results of Voiceprint in different time of day

keep moving without long time stopping. Although, when vehicles stay stationary during the detection period, it may result in false alarms (some complex conditions appear in the urban area such as red light and traffic jam), Voiceprint is still an effective method considering the cost, complexity and performance.

The experiment results of the Sybil attack with power control in different periods of day are shown in Figure 16. Here, $N_{CP}(a)$ is the number of change-points in RSSI time series received from the node a. From these figures, we observe that the malicious node (node 1) cannot be detected by DTW comparison, but it is identified as an illegitimate node via chage-points detection. Based on two proposed detection algorithms, the detection rate of Voiceprint is 100% in both non-peak and peak hours. The false positive rate is 17.4% in peak hours because the traffic congestion makes vehicles moving slowly or keeping almost stationary on the road. If this occurs in the detection period, it is prone to report false alarms about those vehicles who are close to the malicious node. However, the false positive rate is greatly reduced to 1.7% if we confirm a Sybil node after several detection periods.

7 Conclusion

In this paper, we improve Voiceprint to allow it to conduct detection on SCH. This improvement greatly shortens observation time and reduces false positive rate. Moreover, we extend Voiceprint with multiple change-points detection method to find abrupt changes in RSSI time series. Thus, Voiceprint has ability to identify those illegitimate nodes who perform power control during Sybil attacks.

Although we propose a solution for the Sybil attack with power control, it is still a complicated problem when we adopt RSSI-based detection scheme. Therefore, we will continue our work on this direction. In future work, we will analyze behaviors of illegitimate nodes who change their transmission powers to establish power control model for Sybil attack. After that, we will further propose attack models to describe complex Sybil attacks with power control. and find new features to deal with this problem.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China (No.61502394, 61772446, 61572403, 61751208), the National Key Research and Development Program of China (No. 2017YFB1001900), the Fundamental Research Funds for the Central Universities (No. 3102017OQD097), HK PolyU G-UACH.

References

[1] D. Kushwaha, P. K. Shukla, and R. Baraskar, "A Survey on Sybil Attack in Vehicular Ad-hoc Network," *International Journal of Computer Applications*, vol. 98, no. 15, pp. 31–36, 2014.

[2] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil Attack in Vehicular Ad Hoc Network based on Roadside Unit Support," in *Proc. MILCOM*, 2009, pp. 1–7.

[3] P. Bernaola-Galvn, J. Oliver, M. Hackenberg, A. Coronado, P. Ivanov, and P. Carpena, "Segmentation of Time Series with Long-range Fractal Correlations," *The European Physical Journal B*, vol. 85, no. 6, pp. 1–12, 2012.

[4] J. R. Douceur, "The Sybil Attack," in *Proc. IPTPS*, 2002, pp. 251–260.

[5] C. Kumar Karn and C. Prakash Gupta, "A Survey on VANETs Security Attacks and Sybil Attack Detection," *International Journal of Sensors, Wireless Communications and Control*, vol. 6, no. 1, pp. 45–62, 2016.

[6] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis Defenses," in *Proc. ISIPSN*, 2004, pp. 259–268.

[7] M. Raya, P. Papadimitratos, and J. p. Hubaux, "Securing Vehicular Communications," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8–15, 2006.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

[8] C. Chen, X. Wang, W. Han, and B. Zang, "A Robust Detection of the Sybil Attack in Urban VANETs," in *Proc. IEEE ICDCS Workshops*, 2009, pp. 270–276.

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

[10] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP-Sybil Attacks Detection in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582–594, 2011.

[11] K. Mekliche and S. Moussaoui, "L-P2DSA: Location-based Privacy-Preserving Detection of Sybil Attacks," in *Proc. ISPS*, 2013, pp. 187–192.

[12] M. Alimohammadi and A. A. Pouyan, "Sybil Attack Detection Using a Low Cost Short Group Signature in VANET," in *Proc. IEEE ISCISC*, 2015, pp. 23–28.

[13] D. S. Reddy, V. Bapuji, A. Govardhan, and S. Sarma, "Sybil Attack Detection Technique Using Session Key Certificate in Vehicular Ad Hoc Networks," in *Proc. IEEE ICAMMAET*, 2017, pp. 1–5.

[14] M. Demirbas and Y. Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," in *Proc. IEEE WOWMOM*, 2006, pp. 566–570.

[15] S. Lv, X. Wang, X. Zhao, and X. Zhou, "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks," in *Proc. CIS*, vol. 1, 2008, pp. 442–446.

[16] M. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET," *International Journal of Network Security*, vol. 9, no. 1, pp. 22–32, 2009.

[17] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2418–2434, 2010.

[18] R. Shrestha, S. Djuraev, and S. Y. Nam, "Sybil Attack Detection in Vehicular Network based on Received Signal Strength," in *Proc. ICCVE*, 2014, pp. 745–746.

[19] B. Xiao, B. Yu, and C. Gao, "Detection and Localization of Sybil Nodes in VANETs," in *Proc. ACM WDIWAHNSN*, 2006, pp. 1–8.

[20] B. Yu, C. Xu, and B. Xiao, "Detecting Sybil Attacks in VANETs," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, 2013.

[21] M. T. Garip, P. H. Kim, P. Reiher, and M. Gerla, "INTERLOC: An Interference-Aware RSSI-Based Localization and Sybil Attack Detection Mechanism for Vehicular Ad Hoc Networks," in *Proc. IEEE CCNC*, 2017, pp. 1–6.

[22] "IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, March, 2012," *IEEE Std 802.11p-2010*, pp. 1–51, 2010.

[23] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, and P. Mudalige, "Mobile Vehicle-to-Vehicle Narrow-Band Channel Measurement and Characterization of the 5.9 GHz Dedicated Short Range Communication (DSRC) Frequency Band," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1501–1516, 2007.

[24] X. Wang, A. Mueen, H. Ding, G. Trajcevski, P. Scheuermann, and E. Keogh, "Experimental Comparison of Representation Methods and Distance Measures for Time Series Data," *Data Mining and Knowledge Discovery*, vol. 26, no. 2, pp. 275–309, 2013.

[25] S. Salvador and P. Chan, "Toward Accurate Dynamic Time Warping in Linear Time and Space," *Intelligent Data Analysis*, vol. 11, no. 5, pp. 561–580, 2007.

[26] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, "Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs," in *Proc. IEEE/IFIP DSN*, 2017, pp. 591–602.

Yuan Yao (M'13) received the B.S., M.S. and Ph.D. degrees in computer science from Northwestern Polytechnical University, Xian, China, in 2007, 2009 and 2015, respectively. Prior to joining the faculty at NPU, he was a Postdoctoral Researcher in the Department of Computing at Polytechnic University, Hong Kong. He is currently an Associate Professor in the School of Computer Science, Northwestern Polytechnical University. His research interests are in the area of realtime and embedded system, cross-layer design in vehicular ad hoc networks, and security in vehicular networks.

Bin Xiao (S'01-M'04-SM'11) is currently an Associate Professor in the Department of Computing, The Hong Kong Polytechnic University. Dr. Xiao received the B.Sc and M.Sc degrees in Electronics Engineering from Fudan University, China, and Ph.D. degree in computer science from University of Texas at Dallas, USA. His research interests include distributed wireless systems, network security, and software-defined networks (SDN).

Gaofei Wu received the M.S. degree in computer science and technology from the School of Computer, Northwestern Polytechnical University, Xian, China, in 2017. His research interests include vehicular ad hoc networks, embedded system and wireless communications.

Xue Liu (M'06) received the B.S. degree in applied mathematics and the M.E. degree in control theory and applications from Tsinghua University, China, in 1996 and 1999, respectively, and the Ph.D. degree in computer science from the University of Illinois at Urbana-Champaign in 2006. He is currently a Professor in the School of Computer Science at McGill University, Montreal, QC, Canada. His research interests include real-time and embedded systems, performance and power management of server systems, cyber-physical systems.

Zhiwen Yu (S'03-M'06-SM'11) is a Professor from Northwestern Polytechnical University, Xian, China. He was an Alexander Von Humboldt Fellow with Mannheim University, Mannheim, Germany, from 2009 to 2010. He was a Research Fellow with Kyoto University, Kyoto, Japan, from 2007 to 2009. His current research interests include ubiquitous computing and HCI.

Kailong Zhang (M'10) received the B.S., M.S., and Ph.D. degrees from the School of Computer, Northwestern Polytechnical University, Xian, China, all in computer science and technology, with a focus in embedded computing and system design. From 2012 to 2014, he was a Post-Doctoral Researcher with the CyberCars Program, Center of Robotics, Mines ParisTech, Paris, France, where he was involved in the cooperative mechanisms of multiple driverless vehicles. His research interests include the architecture, mechanisms, and design methods for cooperative autonomous embedded system.

Xingshe Zhou (M'04) received the B.S. and M.S. degrees in computer science from Northwestern Polytechnical University, Xian, China. He is a Professor with the School of Computer Science, Northwestern Polytechnical University, Xian, China. He is the Director with Shaanxi Key Laboratory of Embedded System Technology, Xian. His research interests include embedded computing and pervasive computing.