Cross-Layer Scheme for Detecting Large-scale Colluding Sybil Attack in VANETs

Khaled Rabieh¹, Mohamed M. E. A. Mahmoud¹, Terry N. Guo², and Mohamed Younis³

¹Department of Electrical and Computer Eng., Tennessee Tech University, Cookeville, TN 38505 USA
²Center for Manufacturing Research, Tennessee Tech University, Cookeville, TN 38505 USA
³Department of Computer Science and Electrical Eng., University of Maryland Baltimore County, MD 21250, USA

Abstract—In Vehicular Ad Hoc Networks (VANETs), the roadside units (RSUs) need to know the number of vehicles in their vicinity to be used in traffic management. However, an attacker may launch a Sybil attack by pretending to be multiple simultaneous vehicles. This attack is severe when a vehicle colludes with others to use valid credentials to authenticate the Sybil vehicles. If RSUs are unable to identify such an attack, they will report wrong number of vehicles to the traffic management center, which may result in disseminating wrong traffic instructions to vehicles. In this paper, we propose a cross-layer scheme to enable the RSUs to identify such Sybil vehicles. Since Sybil vehicles do not exist in their claimed locations, our scheme is based on verifying the vehicles’ locations. A challenge packet is sent to the vehicle’s claimed location using directional antenna to detect the presence of a vehicle. If the vehicle is at the expected location, it should be able to receive the challenge and send back a valid response packet. The cross-layer design is performed by composing the challenge packet at the MAC layer and directing the PHY layer to send it to the claimed location. Hash function and public key cryptography are used to secure the challenge and response packets. In order to reduce the overhead, instead of sending challenge packets to all the vehicles all the time, packets are sent when there is a suspicion of Sybil attack. We discuss several Sybil attack alarming techniques. The evaluation results demonstrate that our scheme can achieve high detection rate with low probability of false alarm. Additionally, the scheme requires acceptable communication and computation overhead.

Keywords: Location verification, cross layer scheme, Sybil attack, false location reporting attack, and VANET.

I. INTRODUCTION

The current transportation system suffers from series of challenges in terms of high accidents, environmental pollution and efficiency. According to the National Highway Traffic Safety Administration, the number of casualties in car accidents in the U.S. is about 34 thousand in 2012 [1]. Due to recent advances in wireless devices, traffic management applications have emerged to facilitate the communication between smart vehicles. These applications are expected to enhance the current transportation systems by facilitating driving and obviating accidents.

In VANETs, a vehicle communicates with other vehicles and with RSUs. These communications will enable warning drivers in case of emergencies such as traffic congestion and car accidents. Moreover, RSUs need to know the number of vehicles in its vicinity to be used for traffic management. However, the value of VANETs may be void or even becomes negative, i.e., diminishing the road safety, if the network is not well guarded against security attacks. In fact, no responsible government will allow the deployment of VANETs before ensuring that it is completely secure.

Sybil attacks are serious threat where an attacker pretends to be multiple simultaneous vehicles at different locations. This attack is severe when a vehicle colludes with others to use valid credentials to authenticate the Sybil vehicles. We use the term Sybil node to describe non-existing node that attacker claims its presence. If the attacker appears as a few nodes, the attack may not be effective, but large-scale Sybil attacks (where the attacker appear as many Sybil nodes) are more serious in traffic management applications. What makes this attack possible is that each vehicle will be preloaded with many certified pseudonyms and credentials instead of one identity to preserve the driver’s privacy [2]. If each pseudonym is used for a short time and pseudonyms are not linkable, the attackers cannot know any private information about the activities of the vehicle’s driver. However, the abundance of valid identities can be misused to launch Sybil attack by correctly authenticating non-existent vehicles. A very promising approach to detect Sybil attack is by verifying the vehicles’ locations.

In this paper, we propose a cross-layer scheme for detecting large-scale Sybil attack in VANETs. A challenge packet is sent to the vehicle’s claimed location using a directional antenna with beamforming technique. If the vehicle is at the claimed location, it should be able to receive the packet and send back a response packet. The cross-layer design is performed by composing the challenge packet at the MAC layer and directing the PHY layer to send it to a specific location. Hash function and public key cryptography are used to secure the challenge and response packets. In order to reduce the overhead, instead of sending challenge packets to all the vehicles all the time, packets are only sent when there is a suspicion of Sybil attack. We will discuss several attack alarming techniques. Our evaluations demonstrate that our scheme can detect the Sybil vehicles with high accuracy and low probability of false alarms. Moreover, the challenge and response packets are shown to impose acceptable communication and computation overhead.
The main differences between this scheme and existing schemes in the literature can be summarized as follows. The existing schemes such as [3], [4], [5] assume that the vehicle’s identities and credentials are stored in a tamper proof device and thus the attackers cannot collude to use others’ identities. Based on this assumption, these schemes detect Sybil attacks by making sure that each vehicle does not use more than one identity at the same time from its pool of identities. The attack model considered by our scheme is more realistic and harder to counter. We address the case that the adversary can use not only its identities but collude with other vehicles to use their identities as well.

The remainder of the paper is organized as follows. In the next section, we present the network and threat models. In Section III, our Sybil detection attack scheme and Sybil alarming techniques are described in details. The evaluations of the scheme are explained in section IV. We discuss the related work in section V. Finally, Section VI concludes the paper.

II. NETWORK AND THREAT MODELS

A. Network Model

As illustrated in Fig. 1, the considered network model has the following entities.

- **Vehicles**: Vehicles are equipped with GPS and can communicate with each other and with the RSUs. For each vehicle to join the network, it periodically receives a group of pseudonyms, public/private keys, and certificates signed by a trusted certificate authority (CA). Vehicles are not assumed to have tamper proof devices to store the pseudonyms. This not only reduces the cost but also fully trusting these devices will be a vulnerability that can be used by attackers.

- **Roadside unit (RSUs)**: RSUs are access points that are deployed on the roads. They can communicate with each other and with the department of motor vehicle (DMV). They can also communicate with the vehicles. RSUs have directional antenna that is able to focus the radio signals to a narrow area. When RSU detects a Sybil vehicle, it sends an accusation message having the vehicle’s pseudonym to the DMV.

- **DMV**: DMV is responsible for vehicles registration, deployment of RSUs, and ensuring the security of VANETs. When DMV has confidence that a vehicle launches Sybil attack, it asks the certificate authority to revoke the vehicle’s certificates.

- **CA**: CA is responsible for issuing digitally certified pseudonyms to vehicles and revoking them when necessary. Vehicles contact the CA to receive pseudonyms which should be sufficient for a reasonable period of time. Pseudonyms filling can be done during the car annual inspection and registration.

B. Adversary and Threat Model

The DMV and certificate authority are fully trusted because they are operated by the government and thus the security of the VANETs is of their interest. We trust the RSUs in running the Sybil attack detection scheme, but they do not know the real identities of the vehicles. The vehicles are not trusted and may launch Sybil attacks by sending beacon packets for nonexistent vehicles in false locations. Thus, the adversary claims to be several vehicles at false locations. The clocks of the vehicles and the RSUs are synchronized to enable the RSUs to ensure that the packets are fresh. Unlike most of the existing schemes [3], [5], we assume that the attacker not only uses his credentials but can collude with other vehicles to use their credentials.

The Sybil attack can be launched to mislead the vehicles and RSUs in different scenarios. The followings are two example scenarios:

1) An attacker tries to deceive other vehicles that there is a fake accident on the road so that the vehicles change...
Radio transmission at a small area, which is a physical layer technique that can concentrate the vehicle's claimed location. This can be done by beamforming the MAC layer and directs the physical layer to send it to the location as follows. The RSU composes a challenge packet at the claiming location, it verifies the suspected vehicle's vehicles in its communication range. If an RSU suspects of using short-lived pseudonyms and public/private keys. The vehicles without revealing any private information because signed by the vehicle. Beacons can anonymously authenticate time stamp and the vehicle's current location and speed, all hop every 300 ms. From Fig. 4, the beacon has a pseudonym, each vehicle periodically sends a beacon packet over a single stage is out of the scope of this paper. In this section, we first explain our location verification scheme. Then, we explain different Sybil alarming techniques.

A. Location Verification

As shown in Fig. 3, the Sybil attack detection has three stages named alarming, verification and decision. In the alarming stage, several techniques can be used to suspect Sybil attacks. When there is an alarm, the RSU proceeds to the verification stage and performs location verification to assure the vehicles’ claimed position. If the RSU does not find the vehicle at the claimed location, it sends accusation message to the DMV to accuse the vehicle of launching Sybil attack. The DMV is responsible for the decision stage by aggregating the vehicles’ accusations and concluding that the vehicle is launching a Sybil attack if the accusation rate exceeds a threshold. Then, the DMV sends a request to the CA to revoke the accused vehicles’ credentials. Aggregation of the accusations is important to reduce the false positive ratio that may be caused by high signal interference preventing the RSU from receiving the response packet. The details of the decision stage is out of the scope of this paper. In this section, we first explain our location verification scheme. Then, we explain different Sybil alarming techniques.

2) An illustrated in Fig. 2, the attacker tries to deceive the RSU that there is a traffic congestion. If he succeeds, the RSU sends wrong traffic management information to the vehicles. After receiving this information, the victim vehicles change route and clear the road for the attacker.

III. OUR DETAILED SCHEME

As shown in Fig. 3, the Sybil attack detection has three stages named alarming, verification and decision. In the alarming stage, several techniques can be used to suspect Sybil attacks. When there is an alarm, the RSU proceeds to the verification stage and performs location verification to assure the vehicles’ claimed position. If the RSU does not find the vehicle at the claimed location, it sends accusation message to the DMV to accuse the vehicle of launching Sybil attack. The DMV is responsible for the decision stage by aggregating the vehicles’ accusations and concluding that the vehicle is launching a Sybil attack if the accusation rate exceeds a threshold. Then, the DMV sends a request to the CA to revoke the accused vehicles’ credentials. Aggregation of the accusations is important to reduce the false positive ratio that may be caused by high signal interference preventing the RSU from receiving the response packet. The details of the decision stage is out of the scope of this paper. In this section, we first explain our location verification scheme. Then, we explain different Sybil alarming techniques.

A. Location Verification

To comply with the DSRC specifications [6], we assume that each vehicle periodically sends a beacon packet over a single hop every 300 ms. From Fig. 4, the beacon has a pseudonym, time stamp and the vehicle’s current location and speed, all signed by the vehicle. Beacons can anonymously authenticate the vehicles without revealing any private information because of using short-lived pseudonyms and public/private keys.

The RSUs listen passively to all beacons sent from all vehicles in its communication range. If an RSU suspects that there is a Sybil attack, it verifies the suspected vehicle’s location as follows. The RSU composes a challenge packet at the MAC layer and directs the physical layer to send it to the vehicle’s claimed location. This can be done by beamforming which is a physical layer technique that can concentrate the radio transmission at a small area.

2) An illustrated in Fig. 2, the attacker tries to deceive the RSU that there is a traffic congestion. If he succeeds, the RSU sends wrong traffic management information to the vehicles. After receiving this information, the victim vehicles change route and clear the road for the attacker.

III. OUR DETAILED SCHEME

As shown in Fig. 3, the Sybil attack detection has three stages named alarming, verification and decision. In the alarming stage, several techniques can be used to suspect Sybil attacks. When there is an alarm, the RSU proceeds to the verification stage and performs location verification to assure the vehicles’ claimed position. If the RSU does not find the vehicle at the claimed location, it sends accusation message to the DMV to accuse the vehicle of launching Sybil attack. The DMV is responsible for the decision stage by aggregating the vehicles’ accusations and concluding that the vehicle is launching a Sybil attack if the accusation rate exceeds a threshold. Then, the DMV sends a request to the CA to revoke the accused vehicles’ credentials. Aggregation of the accusations is important to reduce the false positive ratio that may be caused by high signal interference preventing the RSU from receiving the response packet. The details of the decision stage is out of the scope of this paper. In this section, we first explain our location verification scheme. Then, we explain different Sybil alarming techniques.

A. Location Verification

To comply with the DSRC specifications [6], we assume that each vehicle periodically sends a beacon packet over a single hop every 300 ms. From Fig. 4, the beacon has a pseudonym, time stamp and the vehicle’s current location and speed, all signed by the vehicle. Beacons can anonymously authenticate the vehicles without revealing any private information because of using short-lived pseudonyms and public/private keys.

The RSUs listen passively to all beacons sent from all vehicles in its communication range. If an RSU suspects that there is a Sybil attack, it verifies the suspected vehicle’s location as follows. The RSU composes a challenge packet at the MAC layer and directs the physical layer to send it to the vehicle’s claimed location. This can be done by beamforming which is a physical layer technique that can concentrate the radio transmission at a small area.

3) An illustrated in Fig. 2, the attacker tries to deceive the RSU that there is a traffic congestion. If he succeeds, the RSU sends wrong traffic management information to the vehicles. After receiving this information, the victim vehicles change route and clear the road for the attacker.

III. OUR DETAILED SCHEME

As shown in Fig. 3, the Sybil attack detection has three stages named alarming, verification and decision. In the alarming stage, several techniques can be used to suspect Sybil attacks. When there is an alarm, the RSU proceeds to the verification stage and performs location verification to assure the vehicles’ claimed position. If the RSU does not find the vehicle at the claimed location, it sends accusation message to the DMV to accuse the vehicle of launching Sybil attack. The DMV is responsible for the decision stage by aggregating the vehicles’ accusations and concluding that the vehicle is launching a Sybil attack if the accusation rate exceeds a threshold. Then, the DMV sends a request to the CA to revoke the accused vehicles’ credentials. Aggregation of the accusations is important to reduce the false positive ratio that may be caused by high signal interference preventing the RSU from receiving the response packet. The details of the decision stage is out of the scope of this paper. In this section, we first explain our location verification scheme. Then, we explain different Sybil alarming techniques.

A. Location Verification

To comply with the DSRC specifications [6], we assume that each vehicle periodically sends a beacon packet over a single hop every 300 ms. From Fig. 4, the beacon has a pseudonym, time stamp and the vehicle’s current location and speed, all signed by the vehicle. Beacons can anonymously authenticate the vehicles without revealing any private information because of using short-lived pseudonyms and public/private keys.

The RSUs listen passively to all beacons sent from all vehicles in its communication range. If an RSU suspects that there is a Sybil attack, it verifies the suspected vehicle’s location as follows. The RSU composes a challenge packet at the MAC layer and directs the physical layer to send it to the vehicle’s claimed location. This can be done by beamforming which is a physical layer technique that can concentrate the radio transmission at a small area.

3) An illustrated in Fig. 2, the attacker tries to deceive the RSU that there is a traffic congestion. If he succeeds, the RSU sends wrong traffic management information to the vehicles. After receiving this information, the victim vehicles change route and clear the road for the attacker.

III. OUR DETAILED SCHEME

As shown in Fig. 3, the Sybil attack detection has three stages named alarming, verification and decision. In the alarming stage, several techniques can be used to suspect Sybil attacks. When there is an alarm, the RSU proceeds to the verification stage and performs location verification to assure the vehicles’ claimed position. If the RSU does not find the vehicle at the claimed location, it sends accusation message to the DMV to accuse the vehicle of launching Sybil attack. The DMV is responsible for the decision stage by aggregating the vehicles’ accusations and concluding that the vehicle is launching a Sybil attack if the accusation rate exceeds a threshold. Then, the DMV sends a request to the CA to revoke the accused vehicles’ credentials. Aggregation of the accusations is important to reduce the false positive ratio that may be caused by high signal interference preventing the RSU from receiving the response packet. The details of the decision stage is out of the scope of this paper. In this section, we first explain our location verification scheme. Then, we explain different Sybil alarming techniques.

A. Location Verification

To comply with the DSRC specifications [6], we assume that each vehicle periodically sends a beacon packet over a single hop every 300 ms. From Fig. 4, the beacon has a pseudonym, time stamp and the vehicle’s current location and speed, all signed by the vehicle. Beacons can anonymously authenticate the vehicles without revealing any private information because of using short-lived pseudonyms and public/private keys.

The RSUs listen passively to all beacons sent from all vehicles in its communication range. If an RSU suspects that there is a Sybil attack, it verifies the suspected vehicle’s location as follows. The RSU composes a challenge packet at the MAC layer and directs the physical layer to send it to the vehicle’s claimed location. This can be done by beamforming which is a physical layer technique that can concentrate the radio transmission at a small area.

3) An illustrated in Fig. 2, the attacker tries to deceive the RSU that there is a traffic congestion. If he succeeds, the RSU sends wrong traffic management information to the vehicles. After receiving this information, the victim vehicles change route and clear the road for the attacker.

III. OUR DETAILED SCHEME

As shown in Fig. 3, the Sybil attack detection has three stages named alarming, verification and decision. In the alarming stage, several techniques can be used to suspect Sybil attacks. When there is an alarm, the RSU proceeds to the verification stage and performs location verification to assure the vehicles’ claimed position. If the RSU does not find the vehicle at the claimed location, it sends accusation message to the DMV to accuse the vehicle of launching Sybil attack. The DMV is responsible for the decision stage by aggregating the vehicles’ accusations and concluding that the vehicle is launching a Sybil attack if the accusation rate exceeds a threshold. Then, the DMV sends a request to the CA to revoke the accused vehicles’ credentials. Aggregation of the accusations is important to reduce the false positive ratio that may be caused by high signal interference preventing the RSU from receiving the response packet. The details of the decision stage is out of the scope of this paper. In this section, we first explain our location verification scheme. Then, we explain different Sybil alarming techniques.

A. Location Verification

To comply with the DSRC specifications [6], we assume that each vehicle periodically sends a beacon packet over a single hop every 300 ms. From Fig. 4, the beacon has a pseudonym, time stamp and the vehicle’s current location and speed, all signed by the vehicle. Beacons can anonymously authenticate the vehicles without revealing any private information because of using short-lived pseudonyms and public/private keys.

The RSUs listen passively to all beacons sent from all vehicles in its communication range. If an RSU suspects that there is a Sybil attack, it verifies the suspected vehicle’s location as follows. The RSU composes a challenge packet at the MAC layer and directs the physical layer to send it to the vehicle’s claimed location. This can be done by beamforming which is a physical layer technique that can concentrate the radio transmission at a small area.
for anomalies. If at least one technique finds an anomaly, the RSU suspects Sybil attack.

**Distance Verification:** To launch effective attack, the attacker should forge many Sybil vehicles with different identities and locations. In this case, it may not be easy for the adversary to dynamically determine valid locations to the Sybil vehicles because the vehicles around the attacker change their locations rapidly and very often. The adversary may mistakenly claim impossible locations for the Sybil vehicles. In this technique, when an RSU receives a beacon packet, it calculates the distance between itself and the location given in the packet. If the distance is greater than the RSU’s maximum communication range [7] or indicates that the vehicle is outside the road, the RSU suspects Sybil attack.

**Location Overlapping:** The attacker can control the false locations sent in the beacons of the Sybil vehicles but he has no control on the co-ordinates sent in the beacons of the benign vehicles. It is possible that a Sybil vehicle’s false location lies in the close proximity of an honest vehicle for some time. In this technique, if an RSU observes such location overlapping, it can suspects Sybil attack. In this case, it should suspect all vehicles that report close positions.

**Vehicles Count:** From the received beacons, each RSU can estimate the number of vehicles passing by. Then, it reports this number to the next RSU in the route. The next RSU compares the number of vehicles it counted to that reported by the previous RSU. If the RSU observes a large increase in the number of vehicles, it can suspect that some vehicles are launching Sybil attack. The effectiveness of this technique depends on the street structures.

**Radio Signal Properties:** Received radio signal strength and angle of arrival are two measurements that is used to suspect Sybil attack [8]. An RSU measures these two radio signal properties and computes approximate coordinates for the transmitter. If the difference between the measured coordinates and the ones reported by the vehicle are more than a threshold, the RSU suspects a Sybil attack.

### IV. EVALUATIONS

#### A. Communication and Computation Overhead

In this section, we evaluate the overhead of the challenge/response packets and pseudonyms. In order to evaluate the computation overhead of the challenge response packets, we have implemented them using Crypto++ library 5.6.0 [9] using a processor Intel core i7 CPU 2.00 GHz and 8 GB RAM. In the simulation, we used 2,048-bit RSA public key cryptography and SHA-2 hash function with 512-bit digest length. For the challenge packet, the RSU verifies the signed beacon and encrypts the pseudonym and a one-time random number. The verification of a beacon takes 0.5 ms and the encryption of the challenge with the public key takes 0.5 ms. Hence, the RSU may take only 1 ms to compose a challenge packet after receiving a beacon. To respond to a challenge packet, the vehicle should decrypt the challenge with its private key and hashes its pseudonym and the one-time random number. Our measurements indicate that the decryption takes 37.61 ms and the hashing takes 0.3 ms. Hence, it takes around 40 ms for the vehicle using the same processor to compose a valid response packet after receiving the challenge packet.

For the communication overhead, we first need to calculate the pseudonyms’ length. To do that, we should estimate the number of pseudonyms used by each vehicle. The total number of pseudonyms that should be loaded in each vehicle is \((N \times D \times T \times 365)\), where \(N\), \(D\) and \(T\) are the number of vehicles in a state, the average driving time for a vehicle in one day in minutes, and the pseudonyms consumption rate (the number of pseudonyms used per minute), respectively. The pseudonym’s size (in bits) can be estimated to be \(\log_2(N \times D \times T \times 365)\). We assume that pseudonyms are distributed once every year. For example, if \(N\), \(D\) and \(T\) are 5 million, 4 hours, and one minute respectively, The total number of pseudonyms used in one year equals 438,000 millions and thus the pseudonym’s size is around 40 bits.

If a vehicle uses one pseudonym every minute, the pseudonyms’ storage area for each vehicle is \(40 \times 4 \times 60 \times 1 \times 365 = 427.73\) KBytes. Public key encryption with a key length of 2,048 bits outputs 2,048 bits for all inputs less than 245 bytes. A challenge packet has a public key encryption and the pseudonym of the vehicle. Assuming that the one-time random number is 40 bits, then the challenge packet’s length is about 261 bytes. The response packet has a pseudonym and a hash value. The length of the response packet is about 69 bytes.

#### B. Security and Performance Evaluations

In our challenge/response mechanism, only the intended vehicle can decrypt the challenge packet’s encryption and obtain the one-time random number. This is because it is infeasible to decrypt the packet without knowing the vehicle’s private key. No one can compose the response packet except the intended vehicle because the one-time random number sent by the RSU is required. Since only the intended vehicle can send a valid response packet, the vehicle is in the claimed location if it can send a valid packet.

In order to assess the effectiveness of the scheme, two performance metrics are considered, namely, prediction rate and false alarm rate. From Fig. 5, the location verification requires transmitting three packets: beacon, challenge, and response. Correspondingly, the road can be divided into three zones: beacon, response, and challenge zones. The challenge zone is near the RSUs and is a small area on the road covered by the RSU’s directional antenna. The vehicle’s antenna at the challenge zone is a regular non-directional antenna. The location verification performance is mainly affected by two factors: the prediction error and packet loss. After receiving the beacon, the RSU estimates when the vehicle enters the challenge zone using the vehicle’s location and speed. The major reasons for packet loss are shadowing and channel collision.

Referring to Fig. 5, let us define the parameters required for performance evaluation.
False alarm rate \( (P_F) \): This is the rate that an honest vehicle is mistakenly accused of reporting false location, given that the beacon packet is received correctly; Detection rate \( (P_D) \): This is the rate of correctly detecting the vehicle that reports false location; \( P \): The probability that a beacon or response packet is received successfully by the RSU from a vehicle in beacon zone or response zone; \( P_0 \): The probability that a challenge packet is received successfully by a vehicle outside the challenge zone; \( P_1 \): The probability that a challenge packet is received successfully by a vehicle outside the challenge zone; \( Q \): The probability that a vehicle enters the challenge zone within the predicted time interval; 

With the assumption that the activities in the three phases are independent, we derive the \( P_F \) and \( P_D \) in the following. For an honest vehicle, the probability that the location verification is correctly performed, given that the beacon packet is successfully received, can be expressed as:

\[
Q P_0 P + (1 - Q) P_1 P. \tag{1}
\]

The first part in (1), \( Q P_0 P \), corresponds to a composite event that the respective vehicle arrives at the challenge zone at predicted time interval and later the response packet is correctly delivered; the second part, \( (1 - Q) P_1 P \), corresponds to a composite event with wrong prediction, successful reception of challenge packet carried by leaking signal outside the challenge zone, and correct delivery of response packet. Note that these two composite events are mutually exclusive. Based on the above discussion, we have the formula for \( P_F \):

\[
P_F = 1 - [Q P_0 + (1 - Q) P_1] P \approx 1 - Q P_0 P, \tag{2}
\]

where the approximation is due to the fact \( P_0 \gg P_1 \approx 0 \).

For the false location reporting attack, exhaustively there are four composite events that are listed in Table I, and the first two are related to \( P_D \) which has a lower bound and an upper bound (Union Bound):

\[
P_D > P \{ \mathcal{E}_1 \} = P(1 - P_1), \tag{3}
\]

\[
P_D \leq P \{ \mathcal{E}_1 \} + P \{ \mathcal{E}_2 \} = P(1 - P_1) + P P_1 (1 - P). \tag{4}
\]

Since \( 1 \gg P_1 \approx 0 \) and \( P \{ \mathcal{E}_2 \} \) is negligible, \( P_D \) is tightly bounded and we can use the middle point of the two bounds as the approximation for \( P_D \):

\[
P_D \approx P(1 - P_1) + P P_1 (1 - P)/2 = P - P P_1 (1 + P)/2. \tag{5}
\]

\( P_F \) and \( P_D \) can be calculated if parameters \( P, P_0, P_1 \) and \( Q \) are given. According to [10], even without considering shadowing effect, packet loss rate can vary dramatically. It is reasonable to consider that each of the parameters has a range. We expect that, with the bounded parameters, \( (P_F, P_D) \) pairs are confined in a limited area. To evaluate \( P_F \) and \( P_D \) performance, we further assume the value of each parameter is a random number following uniform distribution over its range. Fig. 6 shows simulation result based on formulas (2) and (5), with the following parameter ranges: \( P \in [0.91, 0.999], P_0 \in [0.93, 0.9999], P_1 \in [0.0001, 0.01], \) and \( Q \in [0.85, 0.999] \). Each dot in the figure corresponds to a parameter combination and totally 5,000 random combinations are tested. For the parameter ranges specified, \( P_D \) is above 90% and \( P_F \) is most likely in between 5% and 25%. This numerical result suggests that the proposed scheme is quite promising. In addition to the ranges of \( P_D \) and \( P_F \), their distributions can be obtained empirically.

**Table I: All possible composite events related to a false location reporting attack.**

| Composite events | Beacon packet challenge packet Response packet Location verification Note |
|------------------|---------------------------------|-------------------------------|-----------------|-------------------|------------------|
| \( \mathcal{E}_1 \) | received | missed | verified | \* |
| \( \mathcal{E}_2 \) | received | received (due to signal leaking) | missed | verified | \* |
| \( \mathcal{E}_3 \) | received | received (due to signal leaking) | received | failed to verify |
| \( \mathcal{E}_4 \) | missed | – | – | failed to verify |

\* Assume the adversary vehicle is not able to arrive at the challenge zone at expected time interval.
In [3], P2DAP scheme was proposed to detect Sybil attacks. Each vehicle is loaded with a pool of pseudonyms and for every pseudonym, a two-level hash is calculated. Additionally, a collision hash function is applied to group similar pseudonyms into groups. The key of the first-level hash is known to the RSUs and it is used to enable the RSUs to identify the pseudonyms that belong to the same group of vehicles. On the other hand, the key of the second-level hash that can map each pseudonym to an individual vehicle is known only to the DMV. Each time the RSUs overhear pseudonyms of one group, it sends them to the DMV to check whether they belong to different vehicles. A vehicle is accused of Sybil attack when it uses several pseudonyms from its pool to pretend as multiple vehicles.

In [8], Yu et. al, presented a Sybil attack detection approach that uses the received signal strength to verify the physical position of a node. The verifier collects signal strength measurements from its neighbors and calculates the difference between the estimated position and the position announced by the claimer vehicle. Estimated position is calculated based on minimum mean square error. If the difference between the estimated position and the announced one exceeds a threshold, the node is accused of Sybil attack.

In [11], a Sybil attack detection scheme called Footprint is proposed. When a vehicle passes by an RSU, it obtains a signed message as a proof of presence at this location at a certain time. A trajectory of a vehicle is constructed as the vehicle obtains signed messages from different RSUs. Sybil attack can be detected using the fact that the trajectories generated by an attacker are very similar. This scheme is based on the assumption that the probability of two vehicles having the same trajectories is slim. However this assumption is not guaranteed in dense traffic.

In [12], Fogue et. al proposed a proactive cooperative neighbor position and verification scheme based on a message exchange approach. In message exchange, vehicles broadcast anonymous hello messages at random time in the first round. After constant time called guard time, they broadcast a new hello message containing their identity in the second round. Once the message exchange is finished, each vehicle can calculate the distance that separates it from its neighbors by using time of flight based radio frequency ranging. It retrieves the transmission time of the first-round message and the locally stored reception time of the same message to calculate the distance between itself and other neighbors.

In [13], Abu-Elkheir et. al proposed a position verification scheme. Vehicles broadcast beacon messages that have their one-hop neighbors. When a vehicle receives a beacon message, it can know the two-hop neighbors. Vehicles keep the farthest two-hop neighbor location to define a plausible area. To verify a vehicle’s location, the verifier checks if the claimed location lies in the plausible area or not, i.e., the location is farther than the furthest two-hop neighbor or not. The received signal strength is used when the vehicle has no neighbors to verify the sender’s location. If the vehicle has only one-hop neighbors, it can take majority votes of its neighbors to validate a claimed location.

However, the existing schemes assume singular adversary model. Different from them, we address a stronger adversary model assuming that an attacker can collude with other vehicles to use their credentials to authenticate the Sybil nodes.

VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed a cross-layer scheme to detect large-scale Sybil attack in VANETs. We address a strong adversary model assuming that the attacker colludes with others to use valid credentials to authenticate the Sybil vehicles. The MAC layer composes a challenge packet and directs the PHY layer to send it to the expected location using a directional antenna with beamforming technique. If the vehicle is at the expected location, it should be able to send back a valid response packet. We used hash function and public key cryptography to secure the challenge and response packets. In order to reduce the overhead, instead of sending challenge packets to all vehicles all the time, packets are sent when there is a suspicion of Sybil attack. We propose several Sybil attack alarming techniques. Our evaluations have demonstrated that our scheme can detect Sybil attacks with high rate and low probability of false alarm. Moreover the communication and computation overhead of the challenge/response packets are acceptable.

In the future work, we will consider a vehicle-to-vehicle (V2V) Sybil attack detection scheme. The prices of directional antennas is decreasing which can help to equip vehicles with them. Our scheme should enable vehicles to autonomously detect Sybil nodes without any support from RSUs.

REFERENCES
