Detecting Location Spoofing using ADAS sensors in VANETs

Kiho Lim
Department of Computer Science
University of South Dakota
Vermillion SD, USA
kiho.lim@usd.edu

Kastuv M. Tuladhar
Department of Computer Science
University of South Dakota
Vermillion SD, USA
kastuv.tuladhar@coyotes.usd.edu

Hyunbum Kim
Department of Computer Science
University of North Carolina at Wilmington
Wilmington, NC
kimh@uncw.edu

***Abstract*—Location information plays a vital role in vehicular ad-hoc networks (VANETs) as numerous applications are location dependent. Thus, it is essential to preserve the integrity of the location information of vehicles. With the advancement of the vehicular technologies, it is observed that advanced driver-assistance system (ADAS) sensors are being installed on vehicles. In this paper, we propose a detection mechanism of location spoofing by leveraging the on-board ADAS sensors. Under our proposed scheme, attacks based on location spoofing such as sybil attack could be efficiently detected using unique ADAS sensor data like fingerprint, without the involvement of the infrastructure and third party trusted authority.**

Key words: V2V, VANET, location spoofing detection, ADAS sensor, sybil attack.

I. Introduction

In the last few years, we have witnessed the rapid development and deployment of advanced vehicular technology. Various car manufacturers and researchers have been working on the smart vehicle systems, pilot assisted self-driving vehicles towards the fully autonomous driving. Recently, the US Department of Transportation (DOT) has also conducted the connected vehicle (CV) pilot deployment program [1] for real-world feasibility. Vehicular communication has several security requirements as it deals with applications for the safe driving environment such as traffic information, weather condition, road emergency, navigation, value-added-applications etc. Most of, if not all, the above applications relies on the location information. If the location information of vehicles are compromised, then most of the applications will not function properly. Further, false or mis-leaded location information could trigger an accident that can cause financial loss and even threaten drivers' lives [2].

The provision of the on-board GPS has revolutionized the navigation system in driving. Similarly, recent introduction of the short-range radar [3] (radio detection and ranging) and Lidar [4] (light detection and ranging) has provided the virtual eye creating the surrounding map for vehicles and applied as advanced driver-assistance systems (ADAS) to help the navigation and prevent possible accidents by providing the accident awareness warning [5]. Although the advanced sensing technology is leading the vehicles towards connected vehicles and fully autonomous vehicles, the vehicular communication should be protected by possible attackers.

Location is a fundamental and essential information in VANETs, thus a malicious node or attacker can attempt to spread a fake location information to take advantage of finding short routes or to trigger malicious attacks. Some of possible attacks based on location spoofing adversaries can attempt are the following: 1) *Fabrication Attack:* creating a bogus message and lie about the location of traffic congestion or its own location. 2) *Alteration Attack:* Attacker modify the location in the message or its own location information. 3) *Packet Dropping:* Attacker can drop the packets as black-hole attack (dropping all packets) or gray-hole attack (dropping selective packets). 4) *Replay attack:* Attacker pretends to be a vehicle in the past and re-injects the previously received packets or information or beacon messages. 5) *Sybil Attack:* The attacker pretends to be multiple vehicles with fake location information. The attacker may advertise the non-existing neighbors.

In order to address such location spoofing based attacks, various approaches have been studied [6]–[10]. Raya et al. [6] proposed a public-key cryptography scheme to detect and revoke the malicious nodes. The scheme used several pseudonyms for each node where pseudonyms are bind with the private/public key pair issued by the certificate authority (CA). The nodes are revoked by revoking its corresponding certificates. In [11], a scheme to detect a sybil attack was proposed using the resource testing (RT) method in P2P networks. In this method, equal resources are assigned to all the nodes and the attacker has to allocate more resources to its sybil node in order to perform the attack, thus, it cannot behave as a normal node. However, monitoring resource utilization demands separate entity and channel. The modern vehicles perform variety of applications and may requires different resources. Matrucci et al. [7] proposed self-certified pseudonyms to prevent from location spoofing attacks. Authors in [8] proposed a scheme called P^2DAP (Privacy-preserving Detection of Abuses of Pseudonyms). Their scheme consists of two pool of pseudonyms for vehicles. The pools are divided into two hash functions (i.e. coarse-grained and fine-grained). The hash value of the fine-grained pseudonyms are the same for all the pseudonyms of a same node and different for the different nodes. Thus, a roadside unit (RSU) and CA together can verify in case of dispute. Although, pseudonyms fulfill the privacy requirements of the VANET, there is some tradeoff in preserving the anonymity and detecting the location spoofing attacks at the same time.

Park et al. [9] used the TS (time stamps) series to detect the location spoofing attack with the support of RSU. The RSU

978-1-5386-5553-5/19/$31.00 ©2019 IEEE

provides the certificates to the vehicles. With the assumption of two RSUs cannot provide certificates to the same vehicles at the same time, if the two certificates has same TS then it will be treated as a sybil attack. Similarly, in [12], the vehicle location is monitored by gathering the GPS node and collecting position from active neighboring nodes through the signature TS. However, as the scheme relies on the neighbor information, the group of corrupted vehicles can easily circumvent the location verification mechanism. Rabieh et al. [10] proposed cross-layer scheme to detect the sybil attack. The scheme contains a challenge packet to the claimed location of the vehicle. In this scheme, a directional antenna is utilized to communicate in the expected location of the vehicle. However, vehicles may change their speed and trajectory depending on circumstances, further, maintaining the directional antenna for communication is inefficient in VANET as the nodes change their position dynamically. Ruj et al. [13] proposed data-centric misbehavior detection algorithms that detect the false alert messages from the particular location by observing the actions after sending out the alert messages. In this scheme, vehicles send periodic beacon messages so that the neighbors' positions are monitored over the time. The inconsistent position during the alert marks the message as a flag. Similarly, authors in [14] exploited the radar and beacons to crosscheck the location send during the alert message. Golle et al. [15] proposed a scheme to detect misbehaving nodes leveraging the sensor capabilities. The arrived information is validated with the angle of arrival and received signal strength, if mismatched, possible malicious node is suspected. However, the accuracy and efficiency can be elevated by utilizing the advance and accurate sensors. Authors in [16] proposed threshold-based event validation scheme that suspects the malicious nodes on particular location based on counting the number of events reported by multiple vehicles. However, it is possible that multiple vehicles can collude and report the same event message. Further, separate event validating authority is required for all the recorded events.

Most of the above-mentioned approaches require the infrastructure and/or require a third party authority such as the TA to manage and maintain the certificates. In this paper, we propose a scheme for detecting location spoofing attacks without any support from the infrastructure and/or a third part authority. Also, our scheme leverages the existing ADAS sensors installed on vehicles to detect the location spoofing attack, so it does not require any additional hardware cost.

The rest of the paper is organized as follows. Section II introduces the system model of the proposed scheme. Section III presents our proposed scheme in detail. In Section IV, we present the implementation of our scheme and analyze it. Finally, we conclude with discussion and future work in Section V.

II. System Model

In this section, we describe our system model and the assumptions for the proposed protocol and the attacks of interest. In our approach, the locality information of vehicle is utilized to detect the location spoofing attack.

- A wireless transceiver: For the fast and short-range wireless communication, the transceiver of the vehicle adopts the standard dedicated short range communication (DSRC) [17] designed for the VANET standard IEEE802.11p [18]. DSRC for Intelligent Transportation Systems (ITS) is operates in the 5.9 GHz band in the U.S. The range of the transmission is about 250 to 300 meters. We assume that an attacker can modify the location information in messages before transmitting.

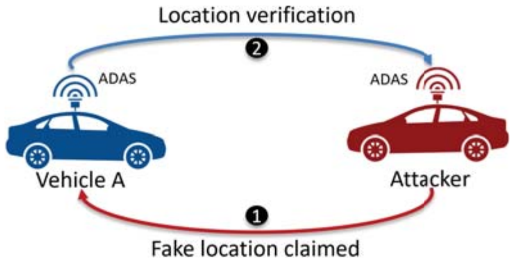

Figure 1: Overview of Location Spoofing Detection

- GPS receiver: To obtain the accurate location, a GPS receiver is used, which provides location information such as latitude, longitude, altitude, speed and the direction of the vehicle. The location provided by the GPS can be fabricated by an attacker but the relative distance and angle of the vehicle can be calculated with the ADAS sensors, thus the location information can be verified.

- ADAS Sensor: Modern vehicles are equipped with the ADAS sensor including radar [3], lidar [4], camera [19] and other sensors such as microwave, infrared or ultrasonic radar. Radar is a low-cost sensor compared to lidar and it offers longer operating distance. Similarly, high resolution cameras are now installed in vehicles that are combined with the image processing, can be utilized to identify the object type. Lidar has been recently used to enable the self-driving car as it can provide continuous 360 degrees of visibility and accurate depth information of the surrounding. We assume a ray-casting lidar is mounted at the top of the vehicle and it generates the frame of the casted points around its surrounding. The frame generated by the ADAS sensors system is in a raw form and it is processed by On-Board-Unit (OBU) of the vehicle. The processed data can find the objects around the vehicle with the distance and angle.

For adversary model, we consider attackers who attempt to launch a location related attack by sending fake position messages. An attacker might fabricate, alter, replay the location related messages or launch a sybil attack. We are interested in the location spoofing attacks which are co-located with the neighboring vehicles traveling along the road. In this paper, we mainly focus on detecting such location spoofing based attacks.

The overview of the location spoofing detection is described in Figure 1. The vehicle equipped with ADAS sensors scans the periphery areas and detects the surrounding objects near the vehicle. The attacker claims the fake position and tries to communicate with the vehicle. The vehicle then verifies if the claimed location is real or fake. To summarize, our main contributions are highlighted as follows:

- A detection scheme that can verify fake location without the presence of a trusted third party and/or an infrastructure in VANET environment.

- Utilization of existing ADAS sensors i.e. lidar, radar, cameras and other on-board sensor units which do not require additional cost.
- A secure and robust protocol against the possible location spoofing attacks.

III. Proposed Scheme

Our proposed scheme uses three main step to detect location spoofing attacks: 1) Source verification; 2) receiver confirmation; 3) surrounding objects verification. We discuss the details of our protocol as follows.

When a vehicle V_R receives a message M with GPS information gps and sensor data $sensor\_data$ from the source vehicle V_S, V_R runs the algorithm for detecting location spoofing as shown in Algorithm 1. To begin the process, V_R checks if the timestamp contained in M is valid and within the threshold τ. If the timestamp is valid, V_R computes the distance d_{RS} and the angle ϕ_{RS} of V_S from V_R using gps information of V_S and V_R. Note that the distance and the angle are computed by leveraging the center point of the target vehicle. For example, if the vehicle is located at (x_1, y_1) and the target vehicle is located at (x_2, y_2) positions, then the distance and angle can be calculated using Equation 1 & Equation 2.

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{1}$$

$$\phi = \tan^{-1}(\frac{y_2 - y_1}{x_2 - x_1}) \tag{2}$$

By using the d_{RS} and ϕ_{RS}, V_R calculates its location and compares it with the $sensor\_data_R$ to see if V_S actually exists at the location where V_S claims to be. If V_S does not exist at the location in $sensor\_data_R$, then location spoofing is detected. The process of source verification is illustrated in the line 6-11 in Algorithm 1. Once the source location is verified, the location of the receiver also needs to be confirmed in the source's sensor data $sensor\_data_S$. Similarly, the distance d_{SR} and the angle ϕ_{SR} of V_R from V_S are computed and the location of V_R is confirmed in $sensor\_data_S$. If the receiver is not found in $sensor\_data_S$, then there exists possible location spoofing. The recipient verification process is illustrated in the line 13-18.

After the locations of source V_S and the receiver V_R are verified, V_R continues to verify the surrounding objects of V_S because the surrounding objects of V_S captured by the ADAS sensor system of V_S should also be captured by the ADAS sensor system of V_R. Note that we assume that the clocks are synchronized and they both use $sensor\_data_R$ and $sensor\_data_S$ generated at the same time ts. To verify the surrounding objects of V_S, V_R generates two objects lists: S_{Li} generated using $sensor\_data_S$ and S'_{Li} generated using $sensor\_data_R$. The objects list contains information such as distance, angle and object type, and the objects are sorted in the order of distance from V_S. Now, V_R compares the distances, the angles, and the objects types between S_{Li} and S'_{Li} and check if the object type is matched and the distance and the angle of the same object is within the error boundary (ϵ_d and ϵ_ϕ). The process of surrounding objects verification is illustrated in line 20-30. Note that it will only check the selected closest objects as V_R might not be able to detect all of surroundings of V_S through its sensors. In this case a similarity score techniques could be used. After the surrounding objects are verified, the algorithm is terminated with location spoofing not detected.

Algorithm 1 Location Spoofing Detection

```
Require: $gps_S, gps_R, sensor\_data_S, sensor\_data_R$
 1: ▷ Check if timestamp is within threshold
 2: if $ts > \tau$ then
 3:     return $FALSE$
 4: end if
 5:
 6: ▷ Source verification
 7: $d_{RS} \leftarrow ComputeDistance(gps_R, gps_S)$
 8: $\phi_{RS} \leftarrow ComputeAngle(gps_R, gps_S)$
 9: if $VerifyObject(d_{RS}, \phi_{RS}, sensor\_data_R)! = V_S$ then
10:     return $FALSE$
11: end if
12:
13: ▷ Recipient confirmation
14: $d_{SR} \leftarrow ComputeDistance(gps_S, gps_R)$
15: $\phi_{SR} \leftarrow ComputeAngle(gps_S, gps_R)$
16: if $VerifyObject(d_{SR}, \phi_{SR}, sensor\_data_S)! = V_R$ then
17:     return $FALSE$
18: end if
19:
20: ▷ Surrounding objects verification
21: $S_{Li} = ComputeObjectList(sensor\_data_S)$
22: $S'_{Li} = ComputeObjectList(sensor\_data_R)$
23: ▷ Compare $S'_{Li}$ with $S_{Li}$
24: for each $L'_i \in L$, $r\phi \leq L_i.\phi' \leq l\phi$ do
25:     if $((L_{i \cdot d} - \epsilon_d \leq L_i.'_d \leq L_{i \cdot d} + \epsilon_d)$ & &
            $(L_{i \cdot \phi} - \epsilon_\phi \leq L_i.\phi' \leq L_{i \cdot \phi} + \epsilon_\phi)$ & &
            $(L_i.'_{type} = L_{i \cdot type}))$ then
26:         $continue$
27:     else
28:         return $FALSE$
29:     end if
30: end for
31: ▷ location spoofing not detected
32: return $TRUE$
```

IV. Implementation & Analysis

In this section, we present the implementation of our scheme and the security analysis. We simulated our scheme using an autonomous urban driving simulator, CARLA [20]. The lidar used in the simulation performs similar to Velodyne HDL-32E and is configured with the following parameters: 32 number of channels, 100 meters of the range, points per seconds (PPS) fixed to 10000, rotating frequency set to 10, field of view (FOV) set to 40°. And the sensor data was collected in the auto-pilot mode.

The simulation environment is shown in the Fig 2 from the Carla simulator that contains the visible objects like target vehicle, trees, trash can, traffic lights etc. The lidar is placed at the vehicle v that sends the pulses of the laser light and scans the object on the basis of the time elapsed by the reflected pulse waves. Note that to cover longer distance and improve accuracy, radar data also can be added, and we consider the objects within 100m in our simulation. By scanning the periphery of the vehicle using ADAS sensor, the surrounding objects including the source vehicle can be identified and the raw data with object detection is shown in the Fig 3.

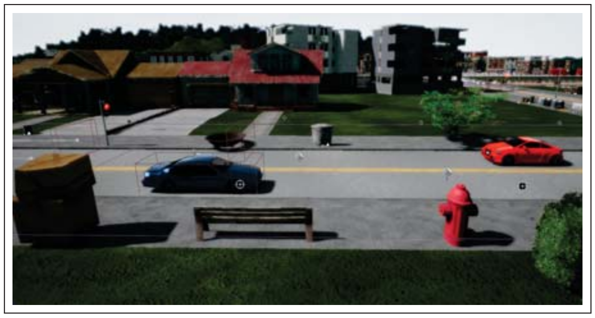

Figure 2: Simulation Environment

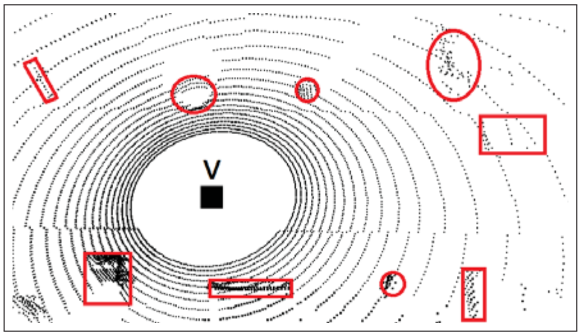

Figure 3: ADAS Sensor Map

To prevent location spoofing attacks, our scheme verifies the location of the source vehicle sending a message by matching the locality information i.e. the distance, angle and the object type near to its surrounding. It consists of the three steps of location verification for the source, the receiver, and the surrounding objects. The location of the vehicle is confirmed by matching the objects in its surrounding. The whole process works like a finger print, i.e., the vehicle has a unique distance and angle towards the surrounding objects from its unique position. This unique sensor information can not be generated unless the vehicle is situated in its claimed location. In VANETs, adversaries may try to attack by fabricating, altering or replaying the location information, but such location spoofing attack can be detected under our scheme.

V. Concluding Remarks & Future Work

VANET application has revolutionized our driving experience. Either it is safety related or entertainment applications, if not all, most of the applications are location aware. In this paper, we introduced our preliminary work to detect the attacks related location spoofing. We explored the different types of location related attacks and proposed a detection mechanism by leveraging the on-board ADAS sensors.

In the future, we will continue to work on our current implementation to improve accuracy and efficiency. For better accuracy on recognizing the surrounding objects and matching them between vehicles, we will utilize machine learning algorithms. Also, we will conduct other location validation tests under different traffic situations to further evaluate our scheme.

References

[1] U. D. of Transportation. (2018) Intelligent transportation systems. [Online]. Available: https://www.its.dot.gov/pilots/

[2] K. Lim and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," *Vehicular Communications*, vol. 4, pp. 30–37, 2016.

[3] Q. Chen, T. Roth, T. Yuan, J. Breu, F. Kuhnt, M. Zöllner, M. Bogdanovic, C. Weiss, J. Hillenbrand, and A. Gern, "DSRC and RADAR object matching for cooperative driver assistance systems," in *Intelligent Vehicles Symposium (IV), 2015 IEEE*. IEEE, 2015, pp. 1348–1354.

[4] B. Schwarz, "Lidar: Mapping the world in 3d," *Nature Photonics*, vol. 4, no. 7, p. 429, 2010.

[5] O. Gietelink, J. Ploeg, B. De Schutter, and M. Verhaegen, "Development of advanced driver assistance systems with vehicle hardware-in-the-loop simulations," *Vehicle System Dynamics*, vol. 44, no. 7, pp. 569–590, 2006.

[6] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, 2007.

[7] L. A. Martucci, M. Kohlweiss, C. Andersson, and A. Panchenko, "Self-certified sybil-free pseudonyms," in *Proceedings of the first ACM conference on Wireless network security*. ACM, 2008, pp. 154–159.

[8] 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.

[9] 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 *Military Communications Conference, 2009. MILCOM 2009. IEEE*. IEEE, 2009, pp. 1–7.

[10] K. Rabieh, M. M. Mahmoud, T. N. Guo, and M. Younis, "Cross-layer scheme for detecting large-scale colluding sybil attack in vanets," in *Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 7298–7303.

[11] J. R. Douceur, "The sybil attack," in *Proceedings of the International workshop on peer-to-peer systems*. Springer, 2002, pp. 251–260.

[12] C. Chen, X. Wang, W. Han, and B. Zang, "A robust detection of the sybil attack in urban vanets," in *Proceedings of the Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on*. IEEE, 2009, pp. 270–276.

[13] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in vanets," in *Proceedings of the Vehicular technology conference (VTC Fall), 2011 IEEE*. IEEE, 2011, pp. 1–5.

[14] R. Hussain, S. Kim, and H. Oh, "Privacy-aware vanet security: Putting data-centric misbehavior and sybil attack detection schemes into practice," in *International Workshop on Information Security Applications*. Springer, 2012, pp. 296–311.

[15] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 2004, pp. 29–37.

[16] H.-C. Hsiao, A. Studer, R. Dubey, E. Shi, and A. Perrig, "Efficient and secure threshold-based event validation for vanets," in *Proceedings of the fourth ACM conference on Wireless network security*. ACM, 2011, pp. 163–174.

[17] J. B. Kenney, "Dedicated short-range communications DSRC standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[18] D. Jiang and L. Delgrossi, "IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments," in *Proceedings of Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*. IEEE, 2008, pp. 2036–2040.

[19] S. Toth, J. Janech, and E. Krsak, "Image recognition system for the vanet," in *Proceedings of the Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on*. IEEE, 2013, pp. 675–678.

[20] A. Dosovitskiy, G. Ros, F. Codevilla, A. Lopez, and V. Koltun, "CARLA: An open urban driving simulator," in *Proceedings of the 1st Annual Conference on Robot Learning*, 2017, pp. 1–16.