Edge Computing based GPS Spoofing Detection Methods

Qian Wang[1], Zhaojun Lu[2], Mingze Gao[1], and Gang Qu[1]

[1]Department of Electrical and Computer Engineering, University of Maryland, College Park, United States
[2]School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan, China
[1]{*qwang126,mgao1,gangqu*}*@umd.edu*
[2]*D201377521@hust.edu.cn*

***Abstract*—Civilian GPS signals are becoming essential for the navigation systems in many applicators such as vehicles and smart phones. However, from a security perspective, GPS signals are vulnerable to the spoofing attacks. Several spoofing detection methods have been proposed, but most of them require extensive signal processing capabilities and additional equipment such as receivers. These add-ons may not be available for vehicles and smart phones. In this paper, we propose a novel edge computing based approach to reconstruct the lost GPS signal. The basic idea is to collect information at the edge nodes and use them to cross-validate the GPS signals received from the satellite. If there is any evidence of spoofing attacks, our method can reconstruct the GPS signal when the signal is unavailable or not trustworthy. Thus, this method could serve as a backup plan to cope with the failure of GPS for the navigation system. Based on real driving data, we can reconstruct the driving routes with an average error of 10 meters and 6 meters by two different methods. This is sufficiently accurate to detect all the simulated GPS spoofing attacks.**

***Index Terms*—Edge Computing, GPS, Spoofing Attacks**

I. Introduction

Nowadays, most of the modern automobiles are equipped with GPS module to assist location relative functions such as smart navigation, emergency assistance, and traffic information service. With the rapid developments of autonomous driving, the algorithms for self-driving rely on the GPS system as a critical fallback to ensure the accurate timing and location. Moreover, as more and more vehicles becoming connected to join the Vehicular Ad-hoc Network(VANET) in assistance of driving, GPS signals have also been widely applied in VANET for precise positioning, message time stamping as well as other real-time network applications[1], [2], [3]. However, from the security perspective, the civilian GPS signals are very vulnerable to outside attackers because they are not encrypted and can easily be spoofed[4]. The GPS spoofing attack could deceive a receiver by broadcasting counterfeit GPS signals that are stronger than the real GPS signals. The same kind of GPS spoofing attacks could also take place on vehicles and this kind of spoofing attacks will cause severe risks on the vehicles because the locations of vehicles are critical and supposed to be reliable and integral for the navigation systems. The situation would become more severe for this attack on the self-driving vehicles because the decisions for autonomous driving highly rely on the sensor data including the position data from the GPS.

Once the GPS signal gets spoofed, the central control system for navigation would be the first to be misled by the malicious attackers. The urgent task for the reliability of the navigation system is to detect the spoofing attacks as soon as possible after the attack took place. There have been several authentications and anti-spoofing techniques for this propose. One of the straightforward methods is to use multiple receivers, i.e, the antennas to cross-check the signal[5], [6]. When adding multiple receivers to check the incoming signals, the slight changes introduced by the spoofed source could be captured by the out of receivers. However, sophisticated attackers could replicate the spoofed signal with phase-aligned to two and more GPS receivers. These sophisticated spoofing attacks are hard to be detected by multi-receivers because it synthesizes spoofing signals for multiple satellites in a way that initially overlays them on top of the true signals. The other methods to detect GPS spoofing leverage on the analysis of the signals as a time of arrival or received strength [7]. While these detection methods would require equipment to capture the characteristics of the signals and may not be flexible on a vehicular system.

As a result, we develop a low-cost validation mechanism for detecting GPS spoofing attacks on vehicles based on the driving information acquired through the in-vehicle Controller Area Network(CAN) bus. Our proposed method relies on the key insight that the data from the inner vehicle network are trusted and demonstrated by the in-vehicle authentication methods[8][9][10]. Our proposed mechanism would detect the spoofing attacks by reconstructing the GPS position from the information recorded on CAN bus, such as the vehicle speed and the steering angle.

This paper makes the following contributions:

1) **A low-cost method**
   Compared to several other approaches proposed to detect the spoofing attacks including the cross-correlation of encrypted signals[5], calibration with multiple antennas[11] and the methods rely on inertial high-stability clocks[7], our cross validation method has significant advantages on the cost. First, our method does not require any extra devices such as the additional antenna or receiver which might be too heavy to carry on and not practical in vehicles. Second, our method

Authorized licensed use limited to: East China Normal University. Downloaded on October 05,2020 at 05:17:14 UTC from IEEE Xplore. Restrictions apply.

focuses on the plain GPS signals and does not need any encryptions and decryptions on the GPS signals. Therefore, our method could avoid aligning with military signals for civilian vehicles which may arouse permission issues on the commercial vehicles. That is because the U.S GPS also includes the military signals that have encrypted on the spreading codes and the legacy code. And those codes can be predicted only with a secret encryption key. Spreading the secret key to civilian vehicles is not applicable.

2) **Trust and validate by the in-vehicle network**
Some methods for positioning rely on the collaboration of the neighbor vehicles in the network, thus arouse the problem of privacy risk for the locations[12]. First, the assisting car might not want to share position to the lost car due to the privacy consideration. Moreover, the assisting car might misbehave to fake false signals to cheat the lost car. Those aroused problems might be solving by the proposed privacy-preserving location, however, need much more efforts to set-up the communications, which will inevitably add influential delays to the system[13]. However, our proposed method uses the local on-board signal which does not need any extra communications from the outside of vehicles. Moreover, the signals collected on board are proved by the in-vehicle authentication communications which are believed to be trusted without any interferences by the third-parties.

3) **Applicable on autonomous vehicles**
As cars become increasingly autonomous, and self-driving vehicles move from the test markets to the main streets, security will become the primary challenge for automakers. The more connected a vehicle is, the more susceptible it becomes to potentially deadly cyber attacks. Our proposed cross-validate method could be applied to the autonomous vehicles with trivial efforts. Besides, autonomous cars take use of a variety of sensors to perceive their surroundings, including radar, laser light, GPS and computer vision modules, which could provide our system with rich sensory data as free of charge.

The remainder of the paper is organized as follows: Section II formally describes our proposed methods in cross-validating the GPS signal with the inner vehicle driving information to detect the spoofing. Section III explains our experiment setup and presents our results that both confirm the reconstruction of the GPS signal and successful detection of spoofing attacks. Section IV concludes the paper.

II. Proposed Approaches

A. Method I: Non-holonomic Car-like Robot Demo (kinematic model)

As previously stated, the main aim of the attacker is to trick the GPS receiver into reporting an inaccurate position without identifying the failure. The first proposed spoofing detection approach leverages the driving information data and the physical model of vehicle. Specifically, the method takes use of the non-holonomic kinematic model to calculate the trajectory of the vehicle and reports the spoofing attacks. The

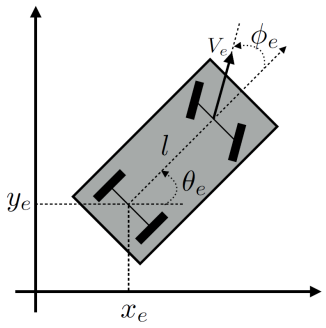

Fig. 1. Generalized Coordinates of a car-like robot

movements of the vehicle can be modeled by the kinematic equations of a car-like robot[14]. The kinematic model is derived from the physical feature of a mobile wheel with the presence of non-holonomic constraints due to the rolling without slipping condition between the wheels and the ground. The symbol of the kinematic model of vehicle is shown in Figure 1. For simplicity, we assume that two wheels on each axle collapse into a single wheel located at the mid-point of the axle. For a front-drive vehicle, we assume that the front wheel can be steered while the rear wheel orientation is fixed. The generalized coordinates are $q = (x, y, \theta, \phi)$, where x and y are Cartesian coordinates of the rear wheel, θ measure the orientation of the car body with respect to the x axis and ϕ is the steering angle. The derived front-wheel driving model is obtained as

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \\ \dot{\phi} \end{bmatrix} = \begin{bmatrix} \cos\theta\cos\phi \\ \sin\theta\cos\phi \\ \sin\phi/l \\ 0 \end{bmatrix} v_1 + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} v_2 \tag{1}$$

Where v_1 is the driving velocity refers to the front wheel and v_2 is the steering velocity input.

Note that the input v_2 in the dynamics is the angle velocity of the wheel, however, our dataset does not provide this measurement. But the dataset has recorded the steering wheel angle status with time stamps which could be used to calculate the steering velocity. Specifically, the steering wheel angle is recorded in degree and the range apart from the normal reference is from -900 degrees to 900 degrees. Based on the mechanical structure of the vehicle, the turning of the steering is proportional to the actual turning of the wheels. Based on vehicle manufacture books, the ratio is varying among different models and it usually falls in between 12:1 to 24:1. Thus, to calculate the dynamics of the vehicle with the steering velocity, we should derive the appropriate steering ratio of the test vehicle. For example, the steering ratio is r and the turning of the steering wheel is Φ, the actual change of the wheel would be $\phi = \Phi/r$. And the angle velocity discussed

Authorized licensed use limited to: East China Normal University. Downloaded on October 05,2020 at 05:17:14 UTC from IEEE Xplore. Restrictions apply.

above can be modeled as $v_2 = \frac{d\phi}{dt}$. The other input of the dynamic functions $v1$ could be acquired directly from the dataset. Each state of vehicle is represented as $q = (x, y, \theta, \phi)$ and the coordinates of the position are calculated by the inputs and the transit state of the function. Based on all the transit states derived from the dynamics equation, the transitory of the vehicle is achieved.

In the kinematic model discussed above, we make approximations when simulating the dynamics of the model. For example, we treat the two wheels as a single axis in the middle but a practical model should also consider the rotation angles of each wheel as generalized coordinates. Furthermore, an accurate model should also account for the presence of actuators and sensors on the wheel axis as well as for typical non ideal such as tire deformation. For example, at higher speeds or with sharp steering, the no-wheel-slip assumption breaks down due to the lateral force. Besides, the above system is assumed to be drift less, i.e, no motion takes place under zero input that there are fewer control inputs than generalized coordinates. But the real road test would be totally different and it is not trivial to establish a complicated mathematical model for the real road condition. Moreover, some parameters to model the dynamics of the vehicle is confidential of the manufacture and not disclosed to the public. As a result, we choose to use the simple one. However, we shall admit the existence of errors when using an approximate model.

B. Method II: Regression Model

As an alternative to mitigate the error generates by approximate modeling, we derive a regressive algorithm to describe the relationship of steering wheel angle and heading of the vehicle. More specifically, we calculate the next coordinates based on the current location, current velocity, and the steering-wheel angle. For example, from the start point, we calculate the next coordinate based on the length of the route (l) and the heading angle (θ). The length of routes can be achieved easily by assuming uniform motion in the small period of time, i.e, $l = v \cdot t$, where v is the sampled velocity of this period and t stands for the time interval. Thus, the corresponding changes could be expressed as the following equations,

$$\begin{cases} \Delta x = l \cos \theta_h \\ \Delta y = l \sin \theta_h \end{cases} \tag{2}$$

Since then, the problem can be formulated as a regression problem to find the relationship of the heading θ_h based on the current and past steering wheel angles. Intuitively, we would think that the steering-wheel controls the heading of the vehicle and it should follow an equation as $\theta_h = f(\theta_w)$. As a result, the key aim of this method is to use regression algorithm in finding the best fit function f and then applying the function to reconstruct the vehicle trajectory. Figure 2 shows the regression results on the heading versus the change of the steering wheel angle. The strict line indicates the linear relationship between the steering and the heading. The spots in the figure are the sampled data from the test drive. By using the function f to calculate the heading of the vehicle, we can construct the next coordinates when plugging into equation (2). One evident advantage of method II is that it avoids the complex states and secrete parameters in method I. Besides, it should be accurate than Method I as it is calculated on empirical data which is not from the approximate formulation.

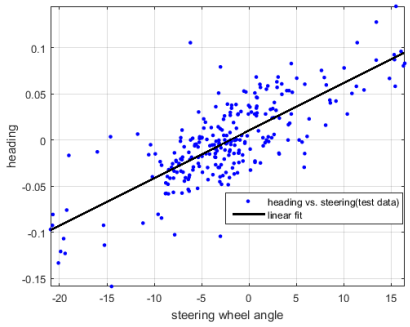

Fig. 2. Regression results on the heading versus steering wheel angle

III. Evaluation Results

Have designed the two methods that use driving information to cross validate the GPS signal and detect any spoofing attacks, we now design a series of experiments to validate our initial hypothesis. First, we collect the driving information as well as the GPS signals from real road tests. Then, we construct the route based on the driving information using the two methods we discussed above. At last, we need to establish whether the cross validation method could detect the GPS spoofing attacks. This can be accomplished by emulating an attack with misleading GPS signals. In following, we execute the detection algorithm and validate the detection rate.

A. Driving Information Data Set

The driving data set we collected from the in-vehicle bus is extremely important to our proposed GPS spoofing detection methods. Here we will shortly introduce the data acquirement methods and the type of data from the set. We acquire the driving data by using the OpenXC platform which is a combination of open source hardware and software that lets the customer extend the vehicle with custom applications and pluggable modules. It uses standard, well-known tools to open up a wealth of data from the vehicle to developers, even beyond OBD-II. OpenXC allows consumer devices, such as smart phones, to access data from any vehicle. Using OpenXC, users can monitor and read out data from many of the sensors on a vehicle, enabling new and innovative vehicle-centric applications. The OpenXC provides a rich dataset including the speed, steering positions, brake positions and the GPS signals from the sensor. This plentiful dataset assists the GPS spoofing detection scheme discussed before.

B. Experimental Results

We now present the results of our experiments, discuss our analysis methodology, and demonstrate how GPS spoofing could be accurately detected. With the OpenXC module assisted, we collect driving data from a real vehicle for 15 routes.

Authorized licensed use limited to: East China Normal University. Downloaded on October 05,2020 at 05:17:14 UTC from IEEE Xplore. Restrictions apply.

The testing routes are designed as 10-20 minutes long with various driving road conditions. With the OpenXC hardware demo plug into the vehicle, we collect the data from the OBD-II board and record it on the cellphone App.

1) Model Validation: The first step is to validate the default parameter of the test vehicle based on the driving data and as well as the GPS signals for reference. For Method I, we achieve the steering ratio r from the test routes in advance. More specifically, we sweep the ratio in the mechanical reasonable range (11-20) in order to find the fitted steering ratio for the test vehicle. Figure 3 displays the constructed routes with a set of ratio values and the real GPS signals (marked in a star) for reference. The figure shows visually the third curve with $r = 13$ is the closest trajectory to the real route. We further narrow down the range and verify the best fit steering ratio of the test vehicle is 12.4. We will use $r = 12.4$ in the following experiments on the GPS spoofing detection.

Similar For Method II, the preliminary step is to model the relationship between the steering and the heading. By using 5000 single data points for training, we derive a linear relationship between the steering and the heading as shown in the Figure 2.

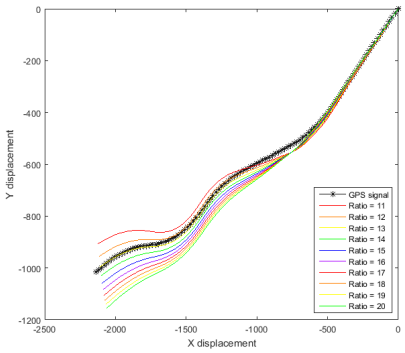

Fig. 3. Routes with different ratio

TABLE I
STATISTICAL RESULTS FROM ROUTE RECONSTRUCTION

Applications	*Method* 1		*Method* 2	
	Max error	**Average error**	**Max error**	**Average error**
route#1	18.03	10.49	13.90	6.95
route#2	19.01	10.67	13.28	6.75
route#3	19.02	10.71	11.73	5.90
route#4	18.68	9.54	12.91	5.58
average	18.57	10.13	12.92	6.25

While we have confirmed that the two methods could construct the trajectory based on the driving information with an accepting error range, we now focusing on constructing our detector. The most important factor of a well-defined detector is the threshold for detection. We would define the threshold by calculating the error between the real GPS signal and the reconstructed locations. More specifically, we evaluate the Euclidean distance error between the constructed route and the location from the GPS signal. To make the signals consistent in formal representation, we map the GPS signal from degrees to relative displacement by calculating the great-circle distance. Therefore, the coordinates of GPS location can be expressed as $P_g(x_g, y_g)$ in meter. Correspondingly, the reconstructed location is expressed as $P_r(x_r, y_r)$. Then, the errors can be defined as $dist(P_r - P_g) = \sqrt{(x_r - x_g)^2 + (y_r - y_g)^2}$. We evaluate the error for route reconstruction by applying the two methods discussed above as shown in Table I. For all the test routes, the average error is 10.13m for Method I and 6.25m for Method II. By considering the route distance from the real road situation, we use 15m as the threshold to detect the spoofing attacks. Note that the maximum error from Method I is above the threshold. To cope with the false alert for Method I, we consider a sequence of 10 consecutive test points above the threshold as a valid detection of spoofing. In addition, the average error of Method II is 6.25m which achieves 38% decrease from the Method I. Therefore, with lower error rate, Method II will achieve better performance in spoofing detection and positioning.

2) GPS Spoofing Detection: With the definition of the valid detector discussed above, we now seek to emulate a GPS spoofing attack and measure the effects. As we stated before, conducting legitimate GPS spoofing attacks is challenging as well as on road test. We, therefore, use the simulated GPS spoofing attacks to test the baseline of our expectations. Our emulated GPS attacks consisted of wrong GPS signals to mislead the vehicle from the correct route. To simulate how real GPS spoofing attacks impact the GPS signals on board, we designed several routes deviate from the real location to simulate the GPS receiver is under spoofing. The speed of the fake routes keeps the same as the one for real route. The attacks would take place at the intersections. For example, when the vehicle turns right, however, the designed spoofing signals indicate it turning left. From Table II, we could find out that the detection accuracy for the simulated spoofing attacks is 100%. And the response time of Method II is a bit faster than Method I because it does not evaluate consecutive points to make a decision. Overall, our results confirm that the faked GPS signal can be detected using construction methods from in-vehicle measurements.

TABLE II
RESULTS OF DETECTION

Applications	**Detection rate**	**Detection time(s)**
Method 1	100%	18
Method 2	100%	15

IV. CONCLUSION

GPS spoofing attacks threaten the confidentiality of the navigation and position applications in vehicles. In this paper, we propose a cross validate a low-cost method for detecting the spoofing of civilian GPS signals received by vehicles. Using driving information collected from the real routes, we demonstrate the ability to detect such GPS spoofing attacks with high accuracy. We believe that our proposed add-ons can easily be included in the future vehicles, and represents the best means of reliability detect such attacks in the short and medium terms.

Authorized licensed use limited to: East China Normal University. Downloaded on October 05,2020 at 05:17:14 UTC from IEEE Xplore. Restrictions apply.

REFERENCES

[1] Zhaojun Lu, Qian Wang, Gang Qu, and Zhenlin Liu. Bars: A blockchain-based anonymous reputation system for trust management in vanets. In *TrustCom/BigDataSE 2018, New York, NY, USA, August 1-3, 2018*. IEEE, 2018.

[2] Zhaojun Lu, Wenchao Liu, Qian Wang, Gang Qu, and Zhenglin Liu. A privacy-preserving trust model based on blockchain for vanets. *IEEE Access*, 2018.

[3] Zhaojun Lu, Gang Qu, and Zhenglin Liu. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Transactions on Intelligent Transportation Systems*, 2018.

[4] Mark L Psiaki and Todd E Humphreys. Gnss spoofing and detection. *Proceedings of the IEEE*, 104(6):1258–1270, 2016.

[5] Brady W O'Hanlon, Mark L Psiaki, Jahshan A Bhatti, Daniel P Shepard, and Todd E Humphreys. Real-time gps spoofing detection via correlation of encrypted signals. *Navigation*, 60(4):267–278, 2013.

[6] Mark L Psiaki, Brady W O'Hanlon, Jahshan A Bhatti, Daniel P Shepard, and Todd E Humphreys. Civilian gps spoofing detection based on dualreceiver correlation of military signals. In *Radionavigation Laboratory Conference Proceedings*, 2011.

[7] Md Tanvir Arafin, Dhananjay Anand, and Gang Qu. A low-cost gps spoofing detector design for internet of things (iot) applications. In *Proceedings of the on Great Lakes Symposium on VLSI 2017*, pages 161–166. ACM, 2017.

[8] Shalabh Jain and Jorge Guajardo. Physical layer group key agreement for automotive controller area networks. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 85–105. Springer, 2016.

[9] Qian Wang, Zhaojun Lu, and Gang Qu. An entropy analysis based intrusion detection system for controller area network in vehicles. In *System-on-Chip Conference (SOCC), 2018 31th IEEE International*. IEEE, 2018.

[10] Kyong-Tak Cho and Kang G Shin. Viden: Attacker identification on in-vehicle networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1109–1123. ACM, 2017.

[11] Jung-Hoon Lee, Keum-Cheol Kwon, Dae-Sung An, and Duk-Sun Shim. Gps spoofing detection using accelerometers and performance analysis with probability of detection. *International Journal of Control, Automation and Systems*, 13(4):951–959, 2015.

[12] Siam U Hussain and Farinaz Koushanfar. Privacy preserving localization for smart automotive systems. In *Design Automation Conference (DAC), 2016 53nd ACM/EDAC/IEEE*, pages 1–6. IEEE, 2016.

[13] Nathaniel Carson, Scott M Martin, Joshua Starling, and David M Bevly. Gps spoofing detection and mitigation using cooperative adaptive cruise control system. In *Intelligent Vehicles Symposium (IV), 2016 IEEE*, pages 1091–1096. IEEE, 2016.

[14] Alessandro De Luca, Giuseppe Oriolo, and Claude Samson. Feedback control of a nonholonomic car-like robot. In *Robot motion planning and control*, pages 171–253. Springer, 1998.

Authorized licensed use limited to: East China Normal University. Downloaded on October 05,2020 at 05:17:14 UTC from IEEE Xplore. Restrictions apply.