GNSS Location Verification in Connected and Autonomous Vehicles Using in-Vehicle Multimodal Sensor Data Fusion

Nicolas Souli1,2, Christos Laoudias1, Panayiotis Kolios1, Christian Vitale1, Georgios Ellinas1,2, Aris Lalos3,4, Jordi Casademont5,6, Pouria Sayyad Khodashenas6, and Petros Kapsalas7

1KIOS Research and Innovation Center of Excellence, University of Cyprus, Nicosia, Cyprus
2Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus
3Electrical and Computer Engineering Department, University of Patras, Rio, Patras, Greece
4Industrial Systems Institute, “ATHENA” Research Centre, Patras, Greece
5Wireless Networks Group, Universitat Politecnica de Catalunya (UPC), Barcelona, Spain
6Software Networks Area, i2CAT Foundation, Barcelona, Spain
7Panasonic Automotive Systems Europe, Frankfurt, Germany

Abstract

Connected and Autonomous Vehicles (CAVs) rely on Global Navigation Satellite Systems (GNSS), e.g., the Global Positioning System (GPS), for the provision of accurate location information for various functionalities including Vehicle-to-Vehicle/Infrastructure (V2V/V2I) communication and self-navigation. However, GNSS-based location awareness is prone to spoofing attacks, where the attacker generates counterfeit satellite signals. This in turn poses a serious threat to the CAV, e.g., car, drone, etc., as well as the surrounding entities. Thus, this threat needs to be detected reliably and mitigated timely to prevent undesired consequences (e.g., damages, casualties, etc.). To this end, this work proposes a location verification solution that leverages in-vehicle sensor readings (e.g., accelerometer, etc.) and Signals of Opportunity (SoO), as an alternative source of location information. In particular, the multimodal sensor data with SoO location measurements are fused by means of a Kalman filter and the estimated fusion-based location is used to verify the location output of the GPS receiver. In case the GPS location deviates considerably from the fusion-based location, then a location spoofing attack is ascertained. Preliminary experimental results with real GPS and sensor data collected with a drone demonstrate the effectiveness of the proposed approach.

Keywords: connected and autonomous vehicle, location spoofing, signals of opportunity, data fusion.

1. INTRODUCTION

As Connected and Autonomous Vehicle (CAV) technology develops, satellite signal jamming and location spoofing attacks will pose a serious threat with a significant impact on the operation of the CAV, including disruptions in Vehicle-to-Vehicle/Infrastructure (V2V/V2I) communication and navigation.

Currently, CAV navigation systems fundamentally rely on GNSS for location awareness. However, GNSS signals are prone to spoofing attacks and may become unreliable, presenting serious hazards for the vehicle and its surrounding entities. Therefore, these shortfalls need to be addressed by techniques that can timely detect spoofing attacks, so as to prevent any undesired consequences of such attacks. Existing works, e.g., [1], focused on providing an accurate location of autonomous vehicles by proposing a position spoofing attack prevention method based on an ad-hoc network of vehicles. It was shown, through simulations, that the proposed scheme could achieve acceptable performance, based on the collaboration between autonomous vehicles to prevent possible spoofing attacks. To our knowledge, there is no solution currently that uses data collected in-situ, i.e., at a vehicle without any collaboration with neighbouring vehicles, for detecting location spoofing attacks.

To this end, this work introduces a location verification solution that combines in-vehicle sensor readings, e.g., data that are readily available from a car’s Controller Area Network (CAN) bus, such as speed, direction, odometry data, etc., and SoOs that are ubiquitous in the environment, as an alternative source of location information. The multimodal sensor data and SoOs are fused using a Kalman filter algorithm, while the fusion-based estimated location is used to detect location spoofing attacks targeting the GNSS location. In case the proposed location verification solution identifies that the GNSS location deviates from the fusion-based location, then a possible spoofing attack is detected. Overall, the contributions of this work are summarized as follows:

- An innovative and low-cost location spoofing detection solution is proposed that does not require any information exchange with surrounding vehicles.
- The proposed solution is validated using real GPS and sensor data collected outdoors with a drone and emulating various spoofing attack scenarios.

The rest of this paper is structured as follows. GPS-free localization using SoOs is outlined in Section 2. The attack detection mechanism in the proposed solution is described in Section 3. Section 4 evaluates the performance of the attack detection solution and presents experimental results, while concluding remarks and directions for future research are provided in Section 5.
2. GPS-FREE LOCALIZATION

As technology evolves towards higher levels of automation, a stable and precise navigation system is becoming an absolute necessity for reliable and efficient navigation [2]. However, GNSS signals frequently become unavailable in the presence of interference (including jamming or spoofing) [3], [4], leading to the exploration of alternative methods for localization, such as SoOs [5]. A Relative Position System (RPS) that relies on SoOs has been presented in our previous work [7] and the proposed localization methodology is illustrated in Figure 1a. Initially, the physical distance between the transmitters sensed in the environment (e.g., radio, TV, Wi-Fi, LTE) and the CAV is computed (using a log-normal signal propagation model). This is necessary to estimate the vehicle’s position employing a multilateration method using the estimated $T_k$ positions prior to the loss of GPS information. Multilateration is a conventional method to calculate the unknown location of a receiver node as discussed in [6], [7]. An Extended Kalman Filter (EKF) is then employed in a multimodal fusion approach to derive the vehicle’s refined location $\hat{x}$ and the measured vehicle system state at time $k$. First, the vehicle’s state at time $k + 1$ is predicted following the adopted vehicle motion model [8]. Subsequently, the predicted position is updated with the estimated SoO-based position to obtain, at each timestamp, the GPS-free vehicle’s location $\hat{x}$.

In this way, a smooth location trajectory can be obtained for the vehicle through the EKF. This work builds upon the RPS solution to output an estimated location data stream for the moving vehicle that is then compared to the GPS location data stream to detect possible location spoofing attacks. Note that the original RPS approach [7] provides relative location coordinates; however, these can be straightforwardly transformed to global coordinates (i.e., using the GPS location prior to the attack), so that the estimated location $\hat{x}$ can be compared directly with the GPS location $x$.

3. ATTACK DETECTION

This section describes how the estimated location data can be utilized for detecting GPS location spoofing attacks. The attack detection mechanism, shown in Figure 1b, takes as inputs the vehicle’s estimated location $\hat{x}$ and the corresponding GPS location $x$. In our baseline proof-of-concept implementation, firstly the Euclidean distance $e_d = ||x - \hat{x}||$ is computed, i.e., the deviation between the two locations. Then, it is checked whether this distance exceeds a predetermined threshold $T_d$, i.e., if the condition $e_d > T_d$ is satisfied, and in this case an attack is detected.

There are various methodologies to set the detection threshold $T_d$ and in the following a simple empirical approach is described for selecting a proper value. Assuming that for an initial time period no attack is present while the vehicle is moving, a time series of $n$ locations $\hat{x}_i$ and $x_i$ is collected, where $i = 1, ..., n$ denotes the number of location samples. Next, the associated distance errors $e_{d,i}, i = 1, ..., n$ are computed, and based on the values the detection threshold can be selected. This is exemplified in Figure 2a, which depicts the $e_d$ curve for $n = 30$. Even though $T_d$ can be set to any value (e.g., $T_d = \max(e_{d,i}), i = 1, ..., n$), there is a performance trade-off later during operation with respect to the correct and false detections in the presence of attacks. On the one hand, if a very low $T_d$ value is selected, then our solution would probably detect all attempts for spoofing the GPS locations; however, the number of false detections when no attack is present would be rather high, thus rendering the proposed solution ineffective. On the other hand, setting $T_d$ to a very high value would decrease the number of false alarms at the expense of increased misdetections, i.e., actual attacks that go undetected, which would degrade the overall detection accuracy. In this work, $T_d$ is defined as the $\alpha$-th percentile of the $e_d$ distance errors in increasing order.

![Figure 1: a) Block diagram of the Relative Position System [7]; b) Proposed attack detection scheme.](image-url)
4. PERFORMANCE EVALUATION

A number of experiments utilizing real GPS location information were conducted to validate the proposed approach. Initially, we introduce the attack model that is used to emulate the location spoofing attack for generating spoofed GPS location data from the original GPS data. In particular, in this work it is assumed that the attacker can inject random noise to disturb the original GPS data. In this sense, the received GPS signal is denoted as \( \mathbf{x} = \mathbf{x} + \mathbf{w} \sim N(\mu, \Sigma) \), where \( \mu \) and \( \Sigma \) are the mean vector and covariance matrix of the Gaussian noise. This is a reasonable model that is capable to capture location spoofing attacks where a naïve attacker can inject white noise to randomly perturb the legitimate GPS readings (i.e., \( \mu = 0 \) and \( \Sigma = 0 \)) or a smart attacker may introduce a small constant bias to the GPS locations (i.e., \( \mu \neq 0 \) and \( \Sigma = 0 \)), so as to gradually steer the vehicle off course, while avoiding detection. Such attacks are feasible when the attacker is within a range of a few tens of meters from the target vehicle with relatively cheap commercial off-the-shelf equipment, i.e., Software Defined Radio (SDR) hardware, amplifier, and antenna, combined with open-source SDR software. In this work, for the collection of the data required for our performance evaluation, a field experiment was initially carried out using various transmission bands and utilizing the proposed RPS [7]. One broadband antenna was mounted on an SDR module on a drone to acquire SoOs over a large frequency spectrum (via HackRF-one SDR) and following a predefined path. The collected dataset contains 30 samples of GPS locations, velocity, orientation, and acceleration that was subsequently stored in an SQL database and then the samples were provided as input to the proposed attack detection solution.

The performance was assessed using a number of metrics, namely Detection Rate (\( DR \)), Misdetection Rate (\( MR \)), and False Detection Rate (\( FDR \)) that are defined as:

\[
DR = \frac{\text{# of detected attacks}}{\text{# of attacked locations}}
\]

\[
MR = \frac{\text{# of attacks missed}}{\text{# of attacked locations}}
\]

\[
FDR = \frac{\text{# of falsely detected attacks}}{\text{# of non attacked locations}}
\]

Initially, the detection threshold \( T_d \) was set as the 90-th percentile of the distance error \( e_d \) in the attack-free scenario and in this case \( T_d = 32 \) meters, as shown in Fig. 2b.

Two different scenarios are examined (see Fig. 3), where specific subsets of the GPS locations \( \mathbf{x} \) are disturbed as a result of the spoofing attack. The attacked GPS locations were emulated using the attack model described above and adding Gaussian noise \( \mathbf{w} \) with \( \mu = [20 \ 20] \) meters and \( \Sigma = \sigma^2 \mathbf{I} \), where \( \sigma = 3 \) meters is the perturbation in each location coordinate. In the first scenario (Fig. 3a), the second half of the GPS locations (i.e., 15 out of 30 locations) were attacked and the results in Fig. 4a indicate that \( DR = 92\% \) and consequently \( MR = 8\% \). In this case, 2 false attack detections were observed in the remaining 15 attack-free locations, i.e., \( FDR = 13.3\% \). In the second scenario (Fig. 3b), a subset of the GPS locations were attacked (5 at the start and 5 at the end) and the results in Fig. 4a illustrate that \( DR = 90\% \) and \( MR = 10\% \). In this case 3 false attack detections were observed in the remaining locations that were not attacked leading to \( FDR = 15\% \). Moreover, Fig. 4b illustrates that a different value of \( T_d \), i.e., \( T_d = 22 \) that corresponds to the 60-th percentile of \( e_d \), can alter the attack detection performance.
providing higher DR, but with the cost of an increased FDR. In the first scenario (Fig. 3a) the results in Fig. 4b indicate that DR=100%, but with 6 false attack detections observed in the remaining 15 locations that were not attacked, i.e., FDR =40%. In the second scenario (Fig. 3b), the results in Fig. 4b illustrate that DR=100% and FDR =45% with 9 false attack detections in the remaining 20 locations.

![Graph](image)

*Figure 4. Performance evaluation in terms of the DR, MR, and FDR metrics: a) Using the 90-th percentile of e₃ as the detection threshold and b) Using the 60-th percentile of e₃ as the detection threshold.*

5. CONCLUSIONS

In this work, an innovative and low-cost attack detection mechanism is presented that can be utilized as an efficient solution against malicious location spoofing attacks on autonomous vehicles. The proposed solution is modular as the RPS module can be substituted with any other positioning solution that provides the absolute location of the vehicle, e.g., using on-board camera and LIDAR sensor information or traditional localization solutions based on wireless networks. We validated our solution through experiments with real data that were used to emulate realistic scenarios of location spoofing attacks, while the preliminary results demonstrate the effectiveness of the proposed approach in detecting location spoofing attacks reliably.

Ongoing work includes exploring the applicability of the attack detection solution in autonomous cars (in the context of the H2020 CARAMEL project), first by using artificial data generated with the CARLA simulator, and then by integrating and testing the solution using the autonomous car platform provided by Panasonic Automotive.

Future work includes the application of the Unscented Kalman Filter (UKF), instead of the EKF, to address the inherent non-linearities in the car mobility and measurements models, thus improving the data fusion and the accuracy of the vehicle’s estimated location. Finally, adaptive techniques for dynamically adjusting the threshold Tₐ according to the current conditions in the field (e.g., varying accuracy of the GPS in urban setups) will be investigated to improve the robustness of attack detection and increase applicability in real-life scenarios.

ACKNOWLEDGEMENTS

This work was supported by the European Union’s H2020 research and innovation programme under CARAMEL project (Grant agreement No 833611). It has also been supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 739551 (KIOS CoE) and from the Government of the Republic of Cyprus through the Directorate General for European Programmes, Coordination and Development.

REFERENCES

[1] J. Song et al., “Secure location verification for vehicular ad-hoc networks,” in *Proc. IEEE GLOBECOM*, 2008.
[2] M. Maaref et al., “Lane-level localization and mapping in GNSS challenged environments by fusing lidar data and cellular pseudoranges,” *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 1, pp. 73-89, 2018.
[3] K. Shamaei and Z. M. Kassas, “LTE receiver design and multipath analysis for navigation in urban environments,” *Navigation*, vol. 65, no. 4, pp. 655-675, 2018.
[4] Z.Z.M. Kassas et al., “I hear therefore I know where I am: Compensating for GNSS limitations with cellular signals,” *IEEE Signal Processing Magazine*, vol. 34, no. 5, pp. 111-124, 2017.
[5] K. Shamaei et al., “Exploiting LTE signals for navigation: Theory to implementation,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2173-2189, 2018.
[6] C. Laoudias et al., “A survey of enabling technologies for network localization, tracking and navigation,” *IEEE Communications Surveys and Tutorials*, vol. 20, no. 4, pp. 3607-3644, 2018.
[7] N. Souli, P. Kolios, and G. Ellinas, “Relative positioning of autonomous systems using signals of opportunity,” in *IEEE 91st Vehicular Techn. Conf. (VTC Spring)*, 2020. (under publication http://arxiv.org/abs/2004.07090).
[8] G. Mao et al., “Design of an extended Kalman filter for UAV localization,” in *Proc. Information, Decision and Control Conference*, pp 224-229, 2007.