Poster: Location Verification and Recovery for Mobile In-Vehicle Applications

Kexiong (Curtis) Zeng[1], Yanzhi Dou[1], Yaling Yang[1], Ranveer Chandra[2]
[1]Dept. of Electrical and Computer Engineering, Virginia Tech; [2]Microsoft Research
[1]{kexiong6, yzdou, yyang8}@vt.edu; [2]ranveer@microsoft.com

1. INTRODUCTION

Location information of vehicles has started to have high value in various mobile applications (valuable shipment tracking, intelligent transportation systems, Waze, Uber etc.). However, current widely-used localization systems are essentially based on wireless signals, which are inherently vulnerable to signal spoofing attacks due to their openness. Attackers have strong incentives to launch location spoofing attacks on these applications to gain benefits and cause chaos, such as surreptitious valuable shipment hijacking, life-threatening intelligent collisions and database manipulation attacks[1].

Existing location verification systems do not work for above scenarios. Because they either require trusted third party, or software and hardware modifications on devices, signals or infrastructure, which are too expensive to implement. Furthermore, some approaches, such as software abstractions for trusted GPS and location crosscheck between multiple wireless localization sources, are also vulnerable to signal spoofing attacks.

This work proposes a novel system, which leverages the correlation between mobile device sensor hints (move, stop, turn, camera image) and location physical features (intersection, stop sign, traffic light, street view etc.), to deliver accurate and timely location verification and recovery for mobile in-vehicle applications. Particularly, our system employs a novel location recovery scheme only using local wireless-independent sensors. Our system is attack-resistant and low-cost, since it is completely wireless-independent, modification-free and infrastructure-independent. The preliminary results indicate impressive performance.

2. DESIGN AND IMPLEMENTATION

In this work, we consider an external attacker who does not have physical access to the victim's device but launches location spoofing attacks remotely. We assume that the victim's device is mounted on the windshield of the vehicle. As shown in Figure 1, our system is composed of an offline module executed on a remote server and an online module deployed in a mobile device. (1) **Offline module**: At first, we collect location physical features from online sources (Google Map) to build up a database. We define

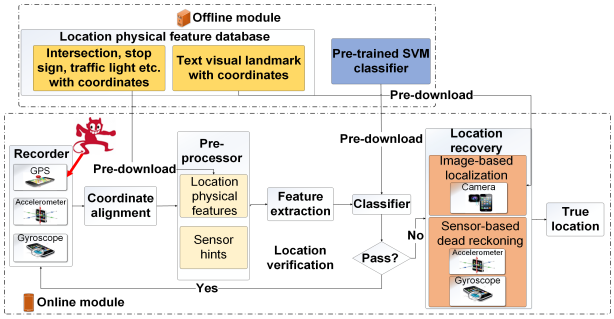

Figure 1: System architecture.

textual information appearing in shop signs, road signs, billboards, building walls etc. as text visual landmarks, which are used for image-based localization. Text visual landmarks with coordinates are extracted by applying OCR (Optical Character Recognition) to online geo-tagged images (Google Street View images). Then, we collect each user's normal driving sensor data and generate anomalous data by replacing real GPS data with falsified GPS data to simulate location spoofing attacks. SVM classifiers with different time window sizes are trained and saved in the user's profile. Finally, the user can download his pre-trained classifiers and location physical features as needed. (2) **Online module**: There are two processes – location verification and location recovery. The location verification process records raw sensor data during a configurable time window, aligns the coordinates of the device and the vehicle, detects sensor hints and compares them with pre-downloaded location physical features. Then, a feature vector is established and fed into the classifier, which returns a result of pass or fail. If it fails location verification, the location recovery process is activated. Image-based localization and sensor-based dead reckoning are combined to recover the true location. Specifically, the device automatically takes pictures of the street view and use OCR to extract textual information, which is compared with the pre-downloaded text visual landmarks for location estimation . Between text visual landmarks, a refined sensor-based dead reckoning is employed.

We implement our system on Android platform and evaluate it with different users in Blacksburg, VA. For location verification, we adopt an adaptive-size time window which grows from 1-min to 5-min with a 1-min step size. The average false negative rates are 51.97%, 35.18%, 18.34%, 2.58%, 4.09% and the average false positive rates are always close to zero. The average detection latency is 134s. For location recovery, the average accumulated localization error is 22m.

3. REFERENCES

[1] N. O. Tippenhauer, K. B. Rasmussen, C. Pöpper, and S. Čapkun. Attacks on public wlan-based positioning systems. In *Proceedings of the 7th international conference on Mobile systems, applications, and services*, pages 29–40. ACM, 2009.

MobiSys'15, May 18–22, 2015, Florence, Italy.
ACM 978-1-4503-3494-5/15/05.
http://dx.doi.org/10.1145/2742647.2745912.