Poster: Towards Quick Angular Check to Rebuff Forged Position Attacks in Vehicular Communication

Yongtae Park and Seungho Kuk
Intelligent Machines Laboratory, Korea University, Republic of Korea
{ytpark, shkuk}@korea.ac.kr

1. MOTIVATION

Although Wireless Access in Vehicular Environment (WAVE) will be legally enforced from 2020 after the recent move by the U.S. Government [1], there is still an unresolved security issue. It is data plausibility, which is not addressed in any standard that comprises the WAVE framework. In particular, an attacker may forge false position values in safety beacons in order to cause unsafe response from startled receiving vehicles. The data plausibility is a longstanding issue for which various approaches based on sensor fusion, behavior analysis and communication constraints have been proposed. However, none of these completely solve the problem.

In this work, we propose an approach in the third category, based on physical constraints of radio communication, to defend against position forgers including stationary roadside attackers. Our approach has certain advantages over the previous approaches. First, it can work even when the sensor-based position check does not work, e.g. in non-line-of-sight (NLoS) condition. This is because most vehicle sensors such as camera, radar, and LiDAR are LoS devices. Second, it can work when the behavioral analysis may fail. For one, the behavioral analysis cannot be applied to a stopped vehicle, since it does not exhibit any movement behavior. Our proposal also departs from existing communication constraints based schemes relying on maximum distance check. This is because the maximum communication distance is a poorly defined variable since it depends on many constantly changing environmental factors and varying transmission power used by the congestion control algorithm. The angle of arrival checking approach is immune to these problems.

2. QUICK ANGULAR CHECK SYSTEM USING ANGLE OF ARRIVAL

In this work, we propose an angle of arrival (AoA) based method to invalidate position forging adversaries such as roadside attackers. Our method is based on the fact that the attacker can falsify the location information of the safety message but cannot lie about the physical location from where the message is transmitted. For example, the relative angle between vehicles can be detected by the AoA of the beacon signal. Therefore, when an attacker tries to induce unsafe reaction from the drivers of the vehicles in its vicinity through the position forgery, it is possible to detect whether the attacker forged its position information by comparing with the measured AoA. Based on the above description, we design a quick angular check system for forgery detection as shown in Fig.1.

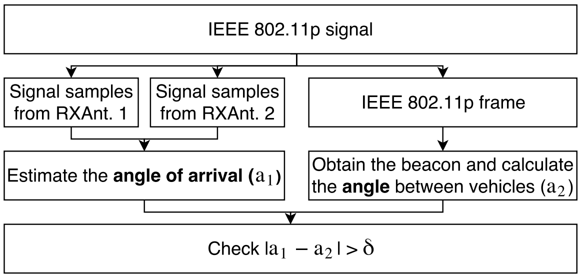
IEEE 802.11p signal
Signal samples from RXAnt. 1
Signal samples from RXAnt. 2
IEEE 802.11p frame
Estimate the **angle of arrival** (a_1)
Obtain the beacon and calculate the **angle** between vehicles (a_2)
Check $|a_1 - a_2| > \delta$

Figure 1: Quick angular check system design

3. PRELIMINARY EVALUATION

We implement a testbed using Chemtronics' On-Board Unit (OBU) and Ettus's Universal Software Radio Peripheral (USRP) B210 with two 5.9 GHz dipole antennas. The USRP B210 allows the use of a synchronized digital signal sample by receiving the safety beacon from the OBU with two antennas. In order to process the digital signal sample, we listen to the WAVE channel using GNU Radio's IEEE 802.11p software on the Linux laptop to detect the short preamble of the beacon and collect signal samples of the following long preamble. The signal samples are analyzed using the MUSIC algorithm that is one of the best AoA estimation methods.

Varying the angle between the OBU and B210, we perform an experiment to measure AoA and compare it with the actual angle. The experimental result shows that more than 96.5% of the measured AoAs have an error within 5 degrees. Based on this, we could confirm that our proposed system can estimate the direction of the actual signal through the AoA, and it is possible to detect messages and attack vehicles that falsify the position except in the same direction.

4. ACKNOWLEDGEMENT

This work was supported by a Korea University Grant.

5. REFERENCES

[1] National Highway Traffic Safety Administration (NHTSA). U.S. DOT advances deployment of Connected Vehicle Technology to prevent hundreds of thousands of crashes. URL: https://www.nhtsa.gov/press-releases/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands, Dec 2016.

MobiSys'17 June 19-23, 2017, Niagara Falls, NY, USA
© 2017 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-4928-4/17/06.
DOI: http://dx.doi.org/10.1145/3081333.3089300