Paper ID EU-TP2228

Using Collective Perception for position verification in VANETs

Tim Leinmüller[1*], Prachi Mittal[2], and Christoph Allig[3]
[1]DENSO AUTOMOTIVE Deutschland GmbH, Germany, t.leinmueller@denso-auto.de
[2]DENSO AUTOMOTIVE Deutschland GmbH, Germany, p.mittal@denso-auto.de
[3]DENSO AUTOMOTIVE Deutschland GmbH, Germany, c.allig@denso-auto.de

Abstract

Sharing of position data is crucial within Vehicular ad hoc Networks (VANETs). It provides the baseline for all safety applications. A security attack involving forged positions can severely harm the vehicles and the passengers. This makes position verification as part of general misbehavior detection a key research activity.

The present paper introduces a novel approach for position verification, complementing existing approaches that we have developed in previous work. The approach makes use of information obtained through collective perception or sensor data sharing. This work describes how to use the information for position verification and discusses merits and shortcomings of such an approach.

Keywords:

Vehicular ad hoc networks (VANETs), Security, Collective Perception, Sensor Data Sharing.

Introduction

Transport and automotive industry have been continuously evolving to make travel safer, more efficient, and generally more intelligent, giving birth to Intelligent Transport System (ITS). Among myriad of concepts within the ITS umbrella, the concept of Cooperative ITS (C-ITS) has been a driving force and a highly researched topic in past decades. C-ITS include vehicles, infrastructure, and a number of other entities that cooperate together to achieve better safety and efficiency within the transport systems. This cooperation, in turn, is achieved by employing communication (mostly direct communication) among the participating entities.

From a vehicle point of view, this communication is termed as Vehicle-to- everything (V2X) communication - short for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. V2X enabled vehicles form highly dynamic networks termed as Vehicular ad hoc Networks (VANETs). These vehicles exchange a variety of data, the most basic of which is ego position data. While the position data is useful, not to say essential for a number of safety, comfort, or efficiency applications, it does come with its own challenges. For example, if a malicious entity (commonly referred to as 'a malicious node') sends forged positions, it can not only rob the vehicles of the benefits of cooperation but also severely endanger the whole network and the vehicles passengers. This makes misbehavior detection in VANETs in form of position verification a key approach for defense.

In this paper, we propose a novel approach for position verification, complementing our previously developed concepts [1]. This approach makes use of information obtained by the concept of sensor data sharing or collective perception where vehicles share with each other the capabilities / characteristics of their sensors and the objects detected using these sensors.

The remainder of this paper is organized as follows. The next section provides background on VANETs and introduces related work. Then, the system model including connected vehicle model and attacker model are presented. The subsequent section presents the novel position verification concepts. Finally, the last section summarizes and concludes the paper.

Technical Background and Related Work

Vehicular Ad Hoc Networks (VANETs)

Vehicular ad hoc networks (VANETs) comprise of vehicles that exchange information over direct communication wireless link. They can be operated using multiple technologies, such as IEEE802.11p [2], referred to as ITS G5 in Europe and Dedicated Short Range Communication (DSRC) in the US, or alternatively LTE-PC5, also referred to as LTE-V2X PC5 or Cellular-V2X (C-V2X) PC5, as specified within 3GPP.

VANETs enable applications aiming at increasing road safety and traffic efficiency. This is achieved by the periodically sharing (broadcasting) a variety of data. Most basic of which is vehicle position data that is transmitted in the form of standardized messages known as Cooperative Awareness Message (CAM) [3] in Europe and Basic Safety Message (BSM) [4] in the US.

Recently, concepts involving a more advanced data exchanged are being discussed. One such concept is of Collective Perception [5, 6] where vehicles share their sensor capabilities and detected objects. At this moment, there is no standard message format for transmission of this data. A so called Collective Perception Message (CPM) is being standardized at the European Telecommunications Standard Institute (ETSI).

Position Verification in VANETs

Misbehavior detection in VANETs has been an active area of research for over a decade. An overview on misbehavior detection in VANETs can be found in the survey from van der Heijden et al. [7].

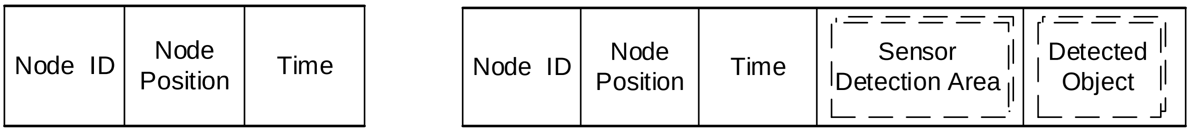
As part of the research on misbehavior detection, multiple approaches for position verification were identified as key defenses against attackers [1, 8, 9].

The present work develops novel position verification approaches using information shared in collective perception messages.

System Model

This section briefly summarizes this work's assumptions with respect to vehicles and their communication and sensing capabilities. Furthermore, it describes the assumed attacker model.

The system consists of vehicles (both connected and not connected) and attackers (mobile or stationary). Without loss of generality, we refrain from considering any other sensor detectable or communicating objects within the scope of this work. Furthermore, for the sake of simplicity, we assume position accuracy to be perfect (no GNSS inaccuracies) and



(a) Beacon Message **(b) Collective Perception Message**

Figure 1 – Simplified Message Formats

neglect vehicle and attacker dimensions. That is, a sensor detected vehicle position matches the same vehicle's position in a CAM or BSM.

Connected Vehicle Model

Connected vehicles are equipped with a short range communication technology (e.g. 802.11p or LTE-PC5) that allows them to directly communicate with other vehicles within a certain communication range (e.g. $500m$). They broadcast periodic beacons (short for beacon messages) containing at least time, their identifier, and their location, as depicted in Figure 1a. Note that this is a simplification of standardized messages such as CAM or BSM.

One vehicle establishes trust in other vehicles through e.g. position verification. The categorization of a vehicle as trusted or untrusted relies on a a framework such as VEBAS [10], where vehicles establish trust over time through position/behavior verification.

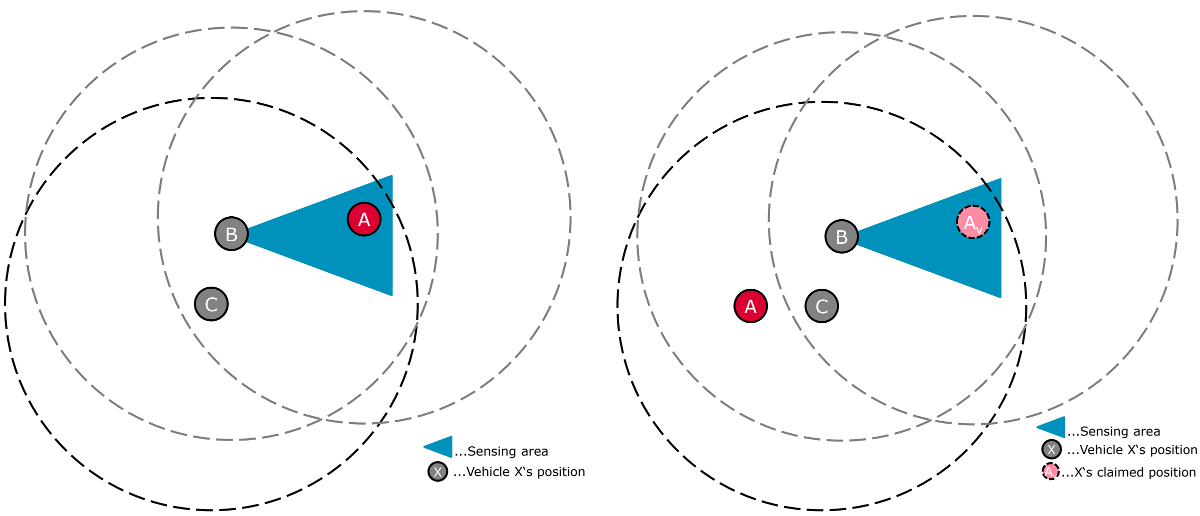
Vehicles equipped with on-board sensors such as camera, radar, or lidar, share information about sensor detected objects in Collective Perception Messages (CPMs). CPMs are distributed (broadcasted) with same or lower frequency than CAMs. Figure 1b shows a simplified structure for a CPM. A CPM includes a list of sensor detection areas of a a vehicle's sensors and a list of all detected (and classified) objects. Within this paper, we assume that a vehicle can match detected objects (that are vehicles) with received beacons from the same vehicle. These objects (vehicles) are included in CPMs and the detected object field indicates that the object (vehicle) was positively matched to a vehicle sending beacons.

If a vehicle is trusted, also the vehicle's on-board sensors and in-vehicle network are assumed to be reliable and trusted. Sensor detected objects (and resulting information in CPMs) are assumed to have higher level of trust than CAMs.

Attacker Model

The attacker model follows the author's previous work in [9, 11]. Differences are that attackers are not limited to being stationary roadside attackers and attackers have the possibility to disseminate CPMs, in addition to CAMs. As a foundation for any kind of attack, main goal of an attacker is to successfully forge position information in its messages to pretend to be at a different location than its real position. To summarize, an attacker is

- Stationary or mobile.
- An insider, i.e. appearing to be a node with a legitimate communication system when sending messages. Note that this means that an attacker has the required security credentials in case the system applies cryptographic means for protection.
- Acting intentionally and actively, i.e. deliberately distributing forged messages.
- Acting alone and not in cooperation with other attackers.
- Capable of creating valid and sound CPMs.



(a) Positive Verification of the Position Claim **(b) Negative Verification of the Position Claim**

Figure 2 – Concept 1: Third Party Position Verification

For the sake of simplicity, this work does not distinguish between single forged positions or forged movements paths and this work assumes that no increase in transmission range is possible.

Position Verification using Collective Perception

CPMs can be used in different ways to verify position information. This work categorizes them in two concepts. The first concept uses CPMs to verify positions claims of third party vehicles. The second concept uses CPMs to verify position claims of the CPM sending vehicle.

It is to be noted that as CPMs are likely send less frequently than beacons. Furthermore, there will be a time delay between consecutive CPMs and beacons, as well as a time delay due to sensor processing. Consequently, the position verification concepts have to employ adequate mechanisms (such as margins and/or interpolation) for compensation.

Third Party Position Verification

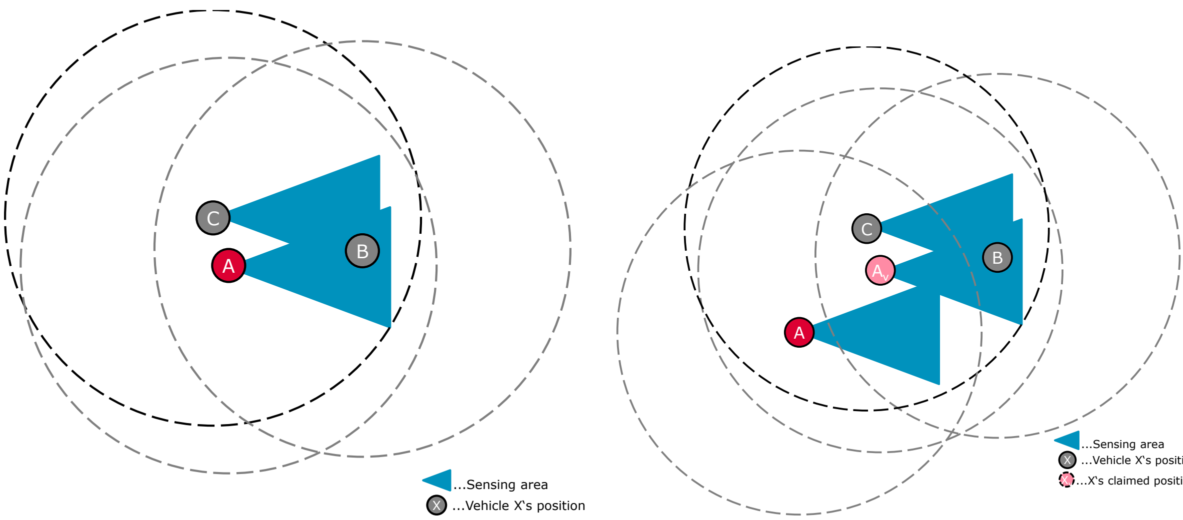
In this case, a vehicle C uses CPMs from a vehicle B to verify position claims of a vehicle A, as depicted in the examples in Figure 2.

In order to be able to apply this concepts, the following prerequisites have to be fulfilled

- B is within C's communication range and B is trusted by C (e.g. through the mechanism from [9])
- B is sending CPMs (in addition to beacons)
- A is sending beacons

A positive position claim verification can be achieved if A is in one of B's sensor detection areas, without any objects blocking the sensor based detection, as shown in Figure 2a. In such cases, B will include A in its CPMs, also indicating that the sensor based detection matches to A's beacons. As a results, this enables C to positively verify the position in A's beacons as well.

The result of the position verification is negative in situations as shown in Figure 2b. Here, A is located at one position, but claiming to be at position A_v in its beacons. Position A_v



(a) Positive Verification of the Position Claim **(b) Negative Verification of the Position Claim**

Figure 3 – Concept 2: CPM Sender Position Verification

lies in one of B's sensor detection areas, again without any object blocking the sensor based detection. Consequently, B's CPM do not include any object at position A_v. Thus, C can conclude that A_v is a forged position claim.

The limitation of this concept is that an attacker within communication range of B would obviously receive B's CPMs. As a consequence, the attacker would be aware of B's sensor detection areas and could avoid detection by only forging position information outside of B's sensor detection area. Nevertheless, even in this case, the concept puts considerable limitations on the attacker's choice of position. And obviously, an attacker never knows if there is yet another vehicle outside of its communication range which has a sensor detection area that covers the attackers forged position.

CPM Sender Position Verification

In the second concept, a vehicle C uses CPMs from a vehicle A to verify vehicle A's position claims in beacons, as shown in the examples in Figure 3.

The prerequisites are as follows

- Vehicle B's position is known to C. Either, because B is present within one of C's sensor detection areas, or/and because C is receiving beacons from B and trusts B.
- A is sending CPMs in addition to beacons.
- A is transmitting beacons (and CPMs) with a position that puts B within one of A's sensor detection areas.

Figure 3a shows an example of a positive position verification. C detects B with its own on-board sensors. The beacons of A contain a position that puts B in one of A's sensor detection areas. A is detecting B with its on-board sensors as well, and consequently including B in its CPMs. As a result, C can positively verify A's position claim, due to the fact they both sense B at the same position.

The corresponding example for a negative verification result is shown in Figure 3b. C detects B with its own on-board sensors. As in the previous attack example, the attacker A is sending beacons claiming to be at position A_v. A is not aware of B (even if B sends beacons, because A and B are not within communication range, as shown in Figure 3b). A is sending CPMs indicating the sensor detection area of A_v, without any object blocking the detection of B. Therefore, A's CPMs do not include B. As a result, C concludes that A must be forging its positions.

The drawbacks of this concept are as follows. As an attacker A can obviously refrain from sending CPMs that might contain incriminating data. If the attacker is sending CPMs, it might create their content in accordance with information that is available from other vehicles' beacons and CPMs. But as for the first concept, this adds limitations on the attackers position forging options and leaves the attacker with an uncertainty of being detected when forging position.

Conclusions

In this paper we introduce two concepts for position verification in VANETs that make use of collective perception / sensor data sharing. The concepts cross-correlate the information in CPMs with a vehicle's information about it's surroundings. If there is a match, the verification is considered positive, if there is a mismatch, it is considered negative.

In the first concept, a vehicle uses CPMs from a second (trusted) vehicle to verify the position claims of a third (hitherto untrusted) vehicle. In the second concept, a vehicle uses CPMs of a hitherto untrusted vehicle itself to verify its position claims. The concepts solely rely on available equipment in vehicles, there needn't be a dedicated verification entity or a dedicated hardware in the vehicles.

After explaining the position verification concepts using true and false position claim examples, we also discuss caveats / limitations of the concepts, where the position verification would fail.

In future work, we plan to validate the above method and concepts with simulations. Beyond the binary positive and negative verification, we envision to take into account varying detection probability of sensors. In addition, we plan to study extending the method to verify parameters other than position (e.g. size, object classification etc).

References

1. T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Decentralized position verification in geographic ad hoc routing," *Security and Communication Networks*, vol. 3, no. 4, pp. 289–302, July/August 2010, (Article first published online: 13. August 2008).
2. IEEE, *IEEE 802.11p-2010 - IEEE Standard for Information technology – Local and metropolitan area networks– Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, IEEE Std., 2010.
3. ETSI, *ETSI EN 302 637-2 V1.3.2 (2014-11) - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, ETSI Std., 2014.
4. SAE, *SAE J2735 200911 - Dedicated Short Range Communications (DSRC) Message Set Dictionary*, SAE Std., 2009.
5. H. Günther, B. Mennenga, O. Trauer, R. Riebl, and L. Wolf, "Realizing collective perception in a vehicle," in *2016 IEEE Vehicular Networking Conference (VNC)*, Dec 2016, pp. 1–8.
6. H. Günther, R. Riebl, L. Wolf, and C. Facchi, "Collective perception and decentralized congestion control in vehicular ad-hoc networks," in *2016 IEEE Vehicular Networking Conference (VNC)*, Dec 2016, pp. 1–8.

7. R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2018.
8. R. Schmidt, T. Leinmüller, and A. Held, "Defending against roadside attackers," in *In proceedings of 16th World Congress on Intelligent Transport Systems*, 2009.
9. T. Leinmüller, R. K. Schmidt, and A. Held, "Cooperative position verification - defending against roadside attackers 2.0," in *Proceedings of 17th ITS World Congress*, 2010.
10. R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *Proceedings of 4th Workshop on Vehicle to Vehicle Communications (V2VCOM 2008)*, 2008.
11. T. Leinmüller, R. K. Schmidt, E. Schoch, A. Held, and G. Schäfer, "Modeling roadside attacker behavior in vanets," in *Proceedings of 3rd IEEE Workshop on Automotive Networking and Applications (AutoNet 2008)*, 2008.