Security Framework for Correct and Secure Positioning in V2X Communication Networks

Oleksandr Mylyy

Hasso Plattner Institute at the University of Potsdam, Prof.-Dr.-Helmert-Strasse 2-3,
14482 Potsdam, Germany
oleksandr.mylyy@student.hpi.uni-potsdam.de

Intelligent vehicles on the roads are already not science fiction but our near future. Vehicles equipped with devices based on short-range wireless communication technologies become enabled for vehicle-to-vehicle or vehicle-to-infrastructure (V2X) communications, often called also Inter-Vehicle communications (IVC). Further, supported with new application systems vehicles can process the received from other vehicles information and become aware of their environment and the traffic situation.

The vehicular networks can be considered as an emerging research area. And if in the near past researchers focused mostly on the problems related to the development of a suitable MAC layer and some limited range of potential applications including such applications as collision avoidance and onboard infotainment services, currently, the security and safety aspects are more and more actively investigated.

Current unsatisfactory traffic-safety statistics contributes to this tendency. Different traffic accidents kill each year approximately 40.000 people on the European Union's (EU) roads. The number of people incurring critical injures and annual costs associated with traffic accidents are also notoriously horrific. In response to these problems, some activities were launched by the governments and manufacturers. Different law prescriptions such as safety-belt laws, antiblocking brake systems (ABS), airbags, and other initiatives improved the road safety situation to some extent, but not enough.

In 2003 the eSafety EU-Initiative was launched as a joint initiative of the European Commission, industry and other stakeholders. The objective was to increase road safety and reduce the number of accidents on Europe's roads. One of the formulated concrete goals was the intention to halve the unacceptably high number of road fatalities up to the year 2010. It is evident, the achievement of this goal is possible only relying heavily on advanced information and communication technologies.

V2X communication networks open doors to a variety of applications for safety, driver assistance, traffic efficiency, and infotainment. Many of these applications rely on accurately determined node locations. The key piece in the exchanged information here is position of a node. Accurate positioning of vehicles yields also accurate navigation which not only increases the road safety but also helps traffic to move more smoothly raising the network performance. However, as open interconnected networks, V2X communication networks are vulnerable to many kinds of attacks. And because algorithms, routing protocols, and applications here mostly use position-based data, this information can be a target of potential attackers. On the other hand, false position information, caused by malfunctioning or non-accuracy of node’s location sensing systems, and distributed in the network, can severely impact the safety and the performance of the network, a successful attack might have catastrophic results, such as the loss of lives. Therefore, the node (vehicle) ability of the verification of the received position and velocity information from other nodes (vehicles) is currently a very challenging problem in V2X communication networks. However, despite the existing position verification approaches, proposed solutions for the problem of position data protection in V2X communication networks cover this problem only to some extent and leave a place for improvements and optimization. The efficiency of the proposed algorithms are mostly estimated using random attackers, the detailed analysis of possible actions of potential attackers and their plausibility has not been provided.

The goal of this work is to develop an effective security framework which enables the providing the efficient plausibility control of distributed position information in V2X communication networks. The internal architecture of the proposed security framework is based on the integration of a set of verification approaches which together with the associated mathematical models create the set of plausibility security sensors, i.e. software modules, containing rules or a priori knowledge that can confirm or disprove a claimed position. We use these sensors based on simple heuristics and experiences, making use of additional data, on reasoning, probabilistic methods and estimation techniques. In order to be able to use significant benefits of sensor fusion, the important task of our research is the evaluation of the results provided by different plausibility security sensors and their efficient usage in the sensor fusion framework. The security sensor fusion and integration process has to be analysed and evaluated as a background for the combination of the plausibility security sensors.

The development of the security framework begins with a detailed analysis of the problem situation and the attacker framework. This analysis comprises:

- discussion about the possible reasons and sources of falsified position information;
- definition and investigation of attackers' scenarios which can be expected in real life;
- attackers' capabilities of data manipulation.

Each manipulation with the position information costs some effort, that means an attacker should always have a specific goal. It can be expected that a potential attacker will not provide unreasoned actions. The best way to convince oneself that malicious actions based on the position information faking can be expected in real life is to define potential attackers and to describe some possible attacker scenarios which could be observed in real life focusing on plausible ultimate goals for such attackers. Several case studies are described and considered as the start point of this research. These scenarios are divided into two classes: right of way advantage and other profits.

Three scenarios belong to the right of way class:

1. The first scenario refers to the highway. In this scenario, an attacker wants to clear his lane tightly occupied by neighbouring vehicles. For that purpose, the attacker sends falsified position information announcing to be ahead with the proposal to change lane because of the observation of a dangerous situation. As a result, the attacker vehicle has the free lane and can accelerate.

2. The next scenario is a well known situation for each driver. When a vehicle enters a highway, it should let through all vehicles which are already on the highway, which in some situations leads to braking and waiting for a possibility to enter the right lane of the highway. In order to avoid this inconvenience the attacker vehicle changes his position information and claims to be a vehicle that is already on the right lane of the highway causing the other neighbouring vehicles decrease their velocities. As a result of this attack, the attacker enters the highway without any trouble. It is important to notice here that the presented scenario is considered in CAR 2 CAR Communication Consortium Manifesto as a possible advantageous option. The ability for all vehicles to share information with each other over a distance adequate to perform the merging manoeuvre can increase the traffic efficiency. We agree to this to some extent. On the highway intervals with a high density manoeuvres which force immediate braking may be not advisable and even dangerous, especially for inexperienced drivers.

3. The last scenario for this class is a city scenario. It depicts a situation where an attacker vehicle does not want to wait its turn on the crossroad and claims to be at a respective position on the crossroad. An opposite vehicle which has the right of way after receiving this notification should brake and let the attacker vehicle through the crossroad without waiting.

Two other scenarios from other profits class describe some additional possible attacker profits:

1. The first scenario, called "witness scenario", describes the situation where an attacker vehicle after observing an accident on the road makes a decision not to stop the vehicle and continues his movement. The goal here is to gain time. But, at the same time the attacker wants to prevent his privacy and avoid accusations problems in the future. For this purpose, the current position is changed with a large enough offset before sending this information to other vehicles in the vicinity. In such a way the attacker imitated a situation as if he had not been there and could not be a witness of the accident.

2. The last considered scenario is dedicated to the very painful question for all drivers. It is not a secret how much time they usually spend to find a free parking place, especially in a big city. The scenario describes a situation where an attacker vehicle after observing a free parking place tries to save it for himself and possibly for his friend or partner. The attacker claims to be in a false position where he is observing a free parking place. As a result, looking for a parking place vehicles are redirected to the wrong place.

For the purpose of the estimation and the evaluation of our security architecture, this work aims at the integration of the position plausibility control methods into the efficient simulation environment for V2X communication networks based on the network simulator ns-2. Real outdoor experiments, which could be used for the evaluation of vehicular protocols, applications, security and efficiency aspects, would require the involvement of a large number of nodes. That is why the simulation of vehicle-to-vehicle communication is also a very challenging topic in recent years. The communication between nodes (vehicles) will be organized using several vehicular broadcasting protocols that have been developed to overcome the constraint of scalability problems by too many vehicles covering too large a distance. Within this work we will develop the basic interfaces between our security framework and these protocols as the basis for integration of these two approaches.