

Integrating Secure Beamforming into Car-to-X Architectures

2011-01-0204

Published
04/12/2011

Hagen Stübing
Adam Opel AG - General Motors Company

Attila Jaeger
Technische Universität Darmstadt

Nikolas Wagner
Adam Opel AG - General Motors Company

Sorin A. Huss
Technische Universität Darmstadt

Copyright © 2011 SAE International

doi: [10.4271/2011-01-0204](https://doi.org/10.4271/2011-01-0204)

ABSTRACT

Intelligent networking of cars and infrastructure (Car-to-X, C2X) by means of dedicated short range communication represents one of the most promising attempts towards enhancement of active safety and traffic efficiency in the near future. Nevertheless, as an open and decentralized system, Car-to-X is exposed to various attacks against security and driver's privacy. This paper presents an approach for enhancing security and privacy on physical layer, i. e., already during sending and receiving of messages. This technique is called Secure Beamforming. In previous works [1], [2] we deployed a simulation-based approach for defining an antenna-array appropriate for most of the safety-related use cases as defined by the Car-to-Car Communication Consortium (C2C-CC).

In this paper we demonstrate a concept for integrating Secure Beamforming into an overall Car-to-X system architecture. The sim^{TD} architecture is thereby taken as the reference architecture because of its detailed specification and near-series alignment. We specify the components and interfaces necessary to enable Secure Beamforming and furthermore define beamforming protocols which are controlling the radiation pattern of the sim^{TD} antennas for a secure sending and receiving of messages.

INTRODUCTION

Intelligent Transport Systems (ITS) based on Car-to-Car Communication and Car-to-Infrastructure Communication (Car-to-X, C2X) are currently moving from a pure research topic towards small-series deployment. Field Operational Tests (FOTs) have been started to examine C2X applications with regard to effects on traffic safety and efficiency. With a vehicle fleet up to 400 vehicles and 100 Road Side Stations (RSU), the German project sim^{TD} is worldwide the first field operational test, large enough to test and validate applications, technologies, and systems for C2X communication in a real-life environment that exceeds the demonstrator status. Sim^{TD} thereby includes various kinds of promising applications from different categories. With respect to road safety, Electronic Brake Light, Collision Avoidance on Intersections or Weather Hazard Warning are applications which may avoid one of the most frequent causes of accidents today. Furthermore, traffic management systems may react on related events more dynamically because mobility data of all vehicles are constantly monitored by RSUs. Traffic assessment becomes more precise and thus, alternative route management becomes more efficient. The multitude of sim^{TD} actors includes vehicles, roadside stations as well as infrastructural facilities for traffic management. Additionally, several third parties are involved to provide access to services and support systems.

Despite all benefits for road safety and traffic efficiency, such a complex and decentralized C2X communication network is highly vulnerable towards data manipulation and eavesdropping of exchanged messages. The consequences for traffic safety resulting from the injection of manipulated or falsified messages are unpredictable. Furthermore, to yield a certain customer acceptance, the tracking of vehicles and inferring of sensitive user data has to be impeded. To thwart such attacks, a comprehensive integration of security and privacy techniques into every C2X architecture is necessary or, in fact, a prerequisite for a successful deployment.

Consequently, the European Telecommunication Standards Institute (ETSI) has settled security¹ as a cross-layer in the ITS reference architecture [3] as depicted in Figure 1. This concludes that every ITS layer is assigned appropriate techniques for securing the data produced on that layer. Similar demands are made for privacy issues. The various layers possess different addressing schemes. Every datagram being part of the final message that may serve as an identifier to track the vehicle has to be included into the identity management.

In sim^{TD} the criticality of security and privacy issues has been recognized and countermeasures have been provided to several layers. In the following we give a brief survey of implemented standards and techniques in sim^{TD} in order to identify open issues and thus to motivate our approach of Secure Beamforming

The IEEE 1609.2 standard [3] is especially developed with respect to communication in wireless vehicular networks. With the main focus on cryptographic techniques this standard proposes a Public Key Infrastructure (PKI) for securing all exchanged C2X messages. Signatures are aimed to authenticate the messages, while the keys used to generate the signatures are certified by Certification Authorities (CA). In sim^{TD} an adapted version of IEEE 1609.2 is deployed as further detailed in [4].

While IEEE 1609.2 ensures message integrity and sender authenticity by means of cryptography, further security techniques based on plausibility checks are applied on the sim^{TD} network layer. In [5] a component has been developed which is capable of verifying the mobility data, i. e., position, speed, and heading inside a message to detect, whether the vehicle is following a realistic driving behavior. Any non-plausible data will be detected and, consequently, marked as insecure.

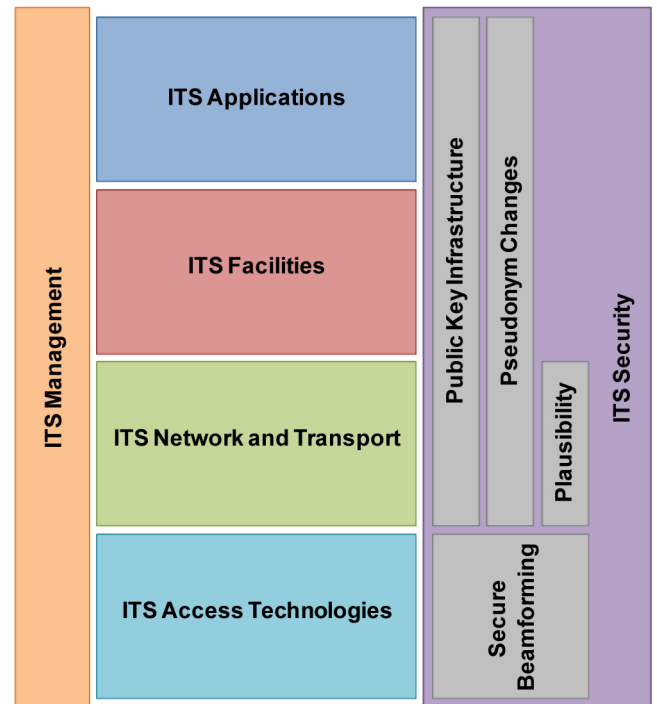


Figure 1. ITS Reference Model

Although there are currently no dedicated standards available for C2X privacy, a commonly accepted concept based on pseudonymity has been established. To reduce linkability, every vehicle possesses several pseudonyms which will be frequently changed according to specified privacy protocols.

In Figure 1 the allocation of security and privacy concepts to the different ITS application layers is illustrated. From there we conclude that, with the exception of the Access Technologies, for every layer security and privacy mechanisms are defined in sim^{TD} . Thus, to fully cover the ITS reference model with security and privacy as required by the standard, appropriate techniques have to be provided for the physical layer, too. This means that privacy and security issues have to be ensured already during the sending and receiving of messages. Motivated by this lack of security within C2X Communication Stack we proposed a physical protection technique called Secure Beamforming [6]. The idea is not to secure the exchanged data only, but to restrict the medium, on which an attacker can operate. By means of radiation pattern control as proposed by [1], ITS stations are able to focus the transmitted energy towards a desired direction by adapting the radiated antenna field so that they may constructively combine in the aimed bearing. In addition, beamforming techniques enable ITS stations to improve signal reception of intended vehicles by rejecting those coming from unwanted directions. When applied appropriately, the adaptive beamforming method on one hand

¹Note that the term Security within the ITS reference models refers to both, data security and privacy whereas, in context of this paper, a distinction between the security concepts is made.

reduces the reception of not trustable messages and on the other it impedes message dissipation into undesired regions. In doing so both goals are reached at the same time: Secure C2X communication with respect to the driver's privacy needs.

The remainder of this paper is organized as follows: The next section presents how the secure beamforming concept was integrated into the sim^{TD} architecture in terms of necessary components and interfaces. In the following section beamforming protocols are proposed which adapt the antenna pattern to realize a secure sending and receiving of messages. The last section summarizes the concepts and gives an outlook on future work.

CAR-TO-X ARCHITECTURE INTEGRATION

According to ETSI [7] and C2C-CC [8] specifications in sim^{TD} vehicles and RSUs are equipped with two separate units. The handling of all communication-related tasks from access up to network and facility layer is performed by the Communication Control Unit (CCU), whereas the Application Unit (AU) hosts all C2X applications for road safety and traffic efficiency. While in [9] a detailed description of the sim^{TD} system architecture is given, we will restrict the presentation to those components relevant for realizing the Secure Beamforming concept. In [Figure 2](#) the architectural composition in terms of components and interfaces is given. The coloring indicates to which communication layer shown in [Figure 1](#) the components refer to.

Applications running on the AU basically perform two consecutive tasks: event detection and event notification. Event detection may thereby include information from local sensors as well from received Car-to-Car messages. After processing and aggregation of the events the application is encapsulating all relevant information into Decentralized Environmental Notification Messages (DENMs). DENMs are event-specific messages and include several fields for network forwarding and event classification. Besides DENMs we focus our study on a further message type generated by the application layer: Probe Vehicles Data (PVD) messages consist of sets of probe values which a vehicle takes while driving (e. g., geographical traces as well as local temperature values). These messages are sent via unicast to a RSU and then forwarded to backend facilities. A more detailed communication analysis is given during the use case study in following sections. The AU Communication Client represents an interface for all incoming and outgoing messages to the CCU. Before passing incoming messages to the applications, the mobility data contained in the messages is verified by the Mobility Data Verification as described in [5].

A major task of the Facility component on the CCU is the creation of Cooperative Awareness Messages (CAMs). CAMs are periodically sent messages including vehicles' mobility data (i. e., position, speed, and heading). These messages, when observed by an adversary, can be used to track a vehicle over longer distances and thus are highly relevant to privacy. In sim^{TD} a sophisticated network layer is deployed which supports most of the forwarding protocols proposed by the C2C-CC [8] (e. g., Contention-based forwarding). For position-based routing a location table is maintained and constantly updated upon newly received messages. Via location services the network layer furthermore may directly query a node position within the network. The C2X Dispatcher obtains the host vehicle's mobility data via a Vehicle Data Provider, which offers access to the CAN bus and GPS module. It assembles the payload with network header and hands over the entire packet to the security component. A signature is then created and the corresponding certificate is added before the message is sent via Access Layer.

Incoming messages are handled by the Ingress Handler. Upon message reception the correctness of the signature and the validity of the certificate are verified. The Location Table is then updated and the forwarding type is evaluated.

The capabilities of Secure Beamforming heavily depend upon the degree of freedom the MAC layers offers for producing situation-based patterns. While in [1] we assumed a very generic antenna aperture, in sim^{TD} only a limited number of different patterns may be produced. The sim^{TD} antenna consists of two software controlled radiators. Each of these produces a semi-circled radiation pattern to the front and to the rear of the vehicle. A per-packet power control is possible for each radiator in steps of 0.5 dB granularity ranging from 0 dBm to 20 dBm [10].

In this work we propose to realize Secure Beamforming as a central component located on the network layer. In [Figure 2](#) solid lines represent already existent communication interfaces, while dotted lines indicate links to be established for integration. The Secure Beamforming component implements the interface of (1) the Vehicle Data Provider, to determine the host vehicles mobility data, (2) the Location Table, to determine the position of relevant receivers and (3) the Security component, to evaluate the trustworthiness of certain receivers. It offers an interface which is integrated by the C2X Dispatcher. Interfacing these components allows precise assessment of the current C2X scenario. With the objectives of enhancing security and privacy, this component determines dynamically the appropriate beamforming for both sending and receiving of messages. In the following sections we give a detailed description of the evaluation scheme executed by the subcomponents Secure Receive and Secure Transmit.