VERIFYING MOBILITY DATA UNDER PRIVACY CONSIDERATIONS IN CAR-TO-X COMMUNICATION

Hagen Stübing[1], Attila Jaeger[2], Norbert Bißmeyer[3], Christoph Schmidt[1], Sorin A. Huss[2]

[1] General Motors Europe, Global Active Safety,
Friedrich-Lutzmann-Ring, 65423 Rüsselsheim, Germany,
{ hagen.stuebing | christoph.schmidt }@gm.com

[2] Technische Universität Darmstadt, Integrated Circuits and Systems Lab,
Hochschulstraße 10, 64289 Darmstadt, Germany,
{ jaeger | huss }@iss.tu-darmstadt.de

[3] Fraunhofer SIT, Secure Mobile Systems,
Rheinstraße 75, 64295 Darmstadt, Germany,
norbert.bissmeyer@sit.fraunhofer.de

ABSTRACT

Inter-vehicle communication and communication between vehicles and infrastructure (Car-to-X, C2X) is a promising technology to improve road safety and driver's convenience. Vehicles create an ad-hoc network with adjacent vehicles or roadside stations in order to transmit messages. These messages may contain warnings of hazardous situations (e.g., hard braking vehicles) or information for traffic efficiency enhancements. All applications using C2X messages rely heavily on the accuracy and reliability of the provided information. Therefore system protection against compromised messages generated by possible attackers or faulty vehicles is a key factor for successful deployment of C2X technology. All messages contain mobility information of the transmitting vehicle. Therefore security mechanisms based on cryptographic primitives may be enhanced by verification mechanisms which evaluate the plausibility of transmitted mobility information.

In this work, we propose a Kalman filter-based approach for efficient mobility verification of neighboring vehicles. The filter is integrated into a verification framework, capable of verifying mobility data even under privacy considerations (i.e. changing pseudonyms). The framework has been developed to fit into an overall C2X system architecture and will be deployed in the context of the project "Safe and Intelligent Mobility Test Field Germany" (sim^{TD})[1], a large scale field operational test for C2X communication. Hence, privacy mechanisms, application support, scalability and performance limitation determined by sim^{TD} are regarded.

[1] See respective project website: http://www.simtd.de

I. INTRODUCTION

Cooperative Intelligent Transport Systems (ITS) networks based on C2X communication are considered as a key technology to achieve the next major breakthrough towards the improvement of active safety and traffic efficiency. By cooperative information interchange, vehicles are able to inform the driver about potential dangerous situations so that she/he may react on time. These systems enable highly promising use cases such as Obstacle, Black Ice, or Full Brake Warning and therefore will contribute to the European Commission policy goals to reduce the currently more than 40,000 road fatalities and more than 2 million accidents on roads every year in Europe[2].

While having started as a research topic, C2X communication is now entering the next phase towards a first deployment of such an ITS by means of a field operational test. The German research project sim^{TD} will put the results of previous research efforts into practice by creating a field trial, large enough to examine the entire spectrum of C2X. For that purpose, sim^{TD} involves several partners from the automotive domain, the telecommunication domain, the German federal state government as well as several universities and research institutes. The sim^{TD} test fleet deploys up to 400 vehicles equipped with a C2X communication system. About 100 vehicles are controlled by hired driver, complemented by approximately 300 free-floating vehicles (e.g., taxis, ambulance cars, commuters, etc.). The sim^{TD} test field is located in and around the city of Frankfurt, Germany and includes motorways, rural and urban roads equipped with up to 100 roadside stations.

Despite all benefits C2X technology contributes to traffic safety and traffic efficiency, such systems are highly vulnerable towards attacks against security and privacy. Potential threats and security requirements have been identified [1][2][3] and countermeasures based on cryptography have been specified [4]. In sim^{TD}, the criticality of security issues has been recognized and a profound integration of these concepts into the overall architecture has been realized [5]. Accordingly, a Public Key Infrastructure (PKI) as specified by [6] has been established. Signatures are responsible for guaranteeing integrity and authenticity of messages while the certificates used to sign the messages are created by the respective sim^{TD} certification authority.

As part of the C2X communication, vehicles in sim^{TD} frequently broadcast their current mobility data in form of so called Cooperative Awareness Messages (CAMs). These CAMs may be observed by an adversary and then used to track the vehicle location, which poses a huge threat to driver privacy. To avoid this, in sim^{TD} each vehicle spontaneously changes all

[2] See respective website: http://ec.europa.eu/transport/road_safety

identifiers that can be used to reconnect the vehicle, e.g., MAC address, IP address, vehicle identifier (ID), and certificate. Such a set of identifiers is called pseudonym [7].

Nevertheless, applying conventional security solutions based on cryptography only ensures message integrity, and authenticity. Thus, an attacker, who has compromised a certificate, will be able to trigger safety critical use cases which may provoke accidents. Hence, to increase the overall security level, further concepts, techniques, and systems are required to verify the message content. In sim^{TD}, application related message content referring to use cases such as Traffic Jam or Black Ice Warning, are verified on higher abstraction layers directly by the respective application. Furthermore, every sim^{TD} message includes mobility data in terms of position, velocity, and heading, which may be verified independently from the application data.

In context of this work, we propose a novel concept for mobility data verification in C2X communication networks. This concept is based on verification techniques as proposed by [8][3] and provides further methods for sophisticated verification of all transmitted mobility information. We advocate a Kalman filter-based approach to estimate a vehicle's future movements, which serve as basis for mobility verification. Taking into account the privacy considerations in sim^{TD}, vehicles may change pseudonyms between subsequent messages, which complicates mobility data verification significantly. Nevertheless, our approach also provides reliable mobility verification in presence of a pseudonym change.

The paper is structured as follows: Section II outlines the sim^{TD} system assumptions and describes the issues addressed within this work. The Kalman filter-based mobility verification as well as its integration into an overall framework is described in detail in section III. In Section IV, implementation details are given and worst case processing times are estimated. Finally, we conclude the paper in section V and give some remarks on future work.

II. ASSUMPTIONS AND SYSTEM REQUIREMENTS

The developed mobility verification framework is embedded into the sim^{TD} vehicle architecture and has to fulfill strong constraints regarding timing and resource consumption in terms of processor load and memory occupation. Furthermore, all relevant system parameter are already determined by the sim^{TD} architecture specification . These are the following:

- CAM messages are sent periodically and include mobility data on the vehicle's position, velocity, and heading. The sending interval of CAM messages is set by congestion control techniques performed on network layer and may vary from 500 ms up to 1000 ms. The maximum transmission range for CAM message is approximately 500 m. This range may be reduced to 250 m in case of channel congestion [9].

- To distribute messages inside the sim^{TD} network, “store & forward” techniques [10] are applied. The proposed verification technique does not verify mobility data which originates from vehicles outside the communication range.

In sim^{TD}, several safety critical messages, which demand instant driver reaction, are exchanged among vehicles within the communication range. For instance, a Full Brake Warning sent by a vehicle driving ahead may cause drivers of subsequent vehicles to adapt their driving behavior accordingly, e.g., by reducing velocity or changing the lane. In case of faked messages, this may have a large impact on traffic safety. Consequently, these messages have to pass a sophisticated security analysis by means of mobility verification.

Our attacker model is based on a static attacker located on roadside [11] as depicted in Figure 1. The attacker is equipped with appropriate sender hardware and is trying to inject faked warning messages. We assume that the attacker has compromised valid sim^{TD} certificates. Therefore, messages sent by this attacker cannot be detected by means of cryptography.

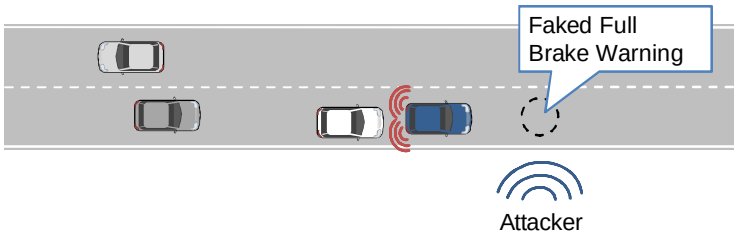

Figure 1: Dangerous Situation Caused by Faked Full Brake Warning

For privacy reasons, changing pseudonyms as illustrated in Figure 2 are suggested. The change of a pseudonym is performed spontaneously. In fact, changing pseudonyms during communication introduces difficulties for sim^{TD} applications such as Intersection Warning whose calculations rely on continuous traces of approaching vehicles. To enable such applications, a pseudonym change has to be made transparent by assigning each vehicle a permanent identifier. It is important to mention that these identifiers are only available for internal application processing and are not available outside the vehicle.

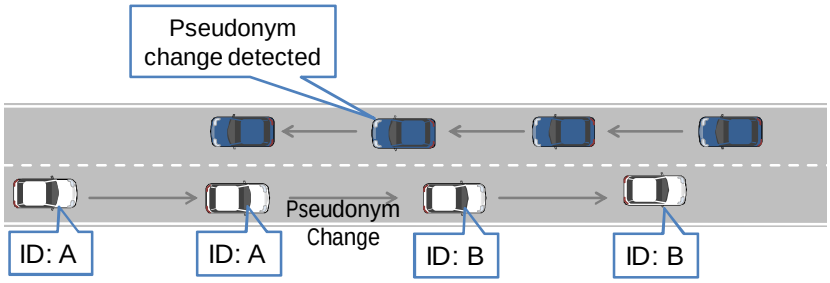

Figure 2: Pseudonym Change Detection

These privacy considerations have an impact on tracking by Kalman filter. In case that a message with unknown vehicle ID has been received, four different possible causes may be identified:

(a) A new vehicle has entered the transmission range,
(b) a vehicle already within transmission range has performed a pseudonym change as depicted in Figure 2,
(c) a vehicle's sender hardware is corrupted, or
(d) an attacker is injecting faked messages as illustrated in Figure 1.

The mobility verification framework has to differentiate between these causes, to perform the evaluation accordingly. Note that from the receiver's point of view, no distinction between reason (c) and (d) is needed.

Under consideration of above stated assumptions and system requirements we developed a framework for vehicle mobility data verification.

III. MOBILITY DATA VERIFICATION APPROACH

In this section a novel verification framework, which is composed of the Kalman filter-based mobility estimator and the corresponding evaluation flow, is proposed. We give a brief introduction into Kalman filter theory and describe its deployment for C2X vehicle tracking. We provide a detailed description how trustworthiness is evaluated and the problem of changing pseudonyms may be solved. Based on these evaluation results, messages will be classified as *Approved*, *Neutral*, or *Erroneous*.

KALMAN FILTER-BASED VEHICLE TRACKING

A Kalman filter is a well known tool for predicting the state of linear dynamic systems based on a series of noisy measurement data. Especially for object tracking, a Kalman filter represents an effective while easily realizable solution [12]. The Kalman filter will generate an optimal prediction, if the measurement error is Gaussian distributed. Indeed, this is the case for position data delivered in sim^{TD}. For these reasons, a Kalman filter seems to be an appropriate approach for our purpose.

In Figure 3 the schematic and corresponding equations for a Kalman filter are depicted. Vehicle tracking is performed within two successive phases repeated for every time step k:

1. Prediction: Next state $\hat{x}_k$ is calculated based on the last state prediction $\hat{x}_{k-1}^{+}$ using an appropriate vehicle mobility model F_k. In addition to the transmitted mobility data $\tilde{y}_k$, i.e., longitude, latitude, heading, and velocity, the Kalman filter also predicts acceleration and yaw rate. Hence, the state vector $\hat{x}_k$ consists of additional elements. That way the

prediction accuracy is improved significantly. Additionally, the predicted accuracy P_k of $\hat{x}_k$ is calculated taking into account system fault variances Q_k, which represent the inaccuracies of the used mobility model.

2. Correction: As indicated previously, the notation form of the system state $\hat{x}_k$ differs from the notation of received mobility data $\tilde{y}_k$. To achieve consistency, the transformation matrix H_k has to be applied to yield $\hat{y}_k$. The difference Δ_k between predicted and received mobility data is calculated. This difference, weighted with Kalman Gain K_k, is used to correct the current system state $\hat{x}_k$ leading to improved state $\hat{x}_k^+$. Thereby, Kalman Gain is determined out of measurement variance R_k, as well as the predicted accuracy P_k. Furthermore also P_k is improved to P_k^+ with regards to K_k.

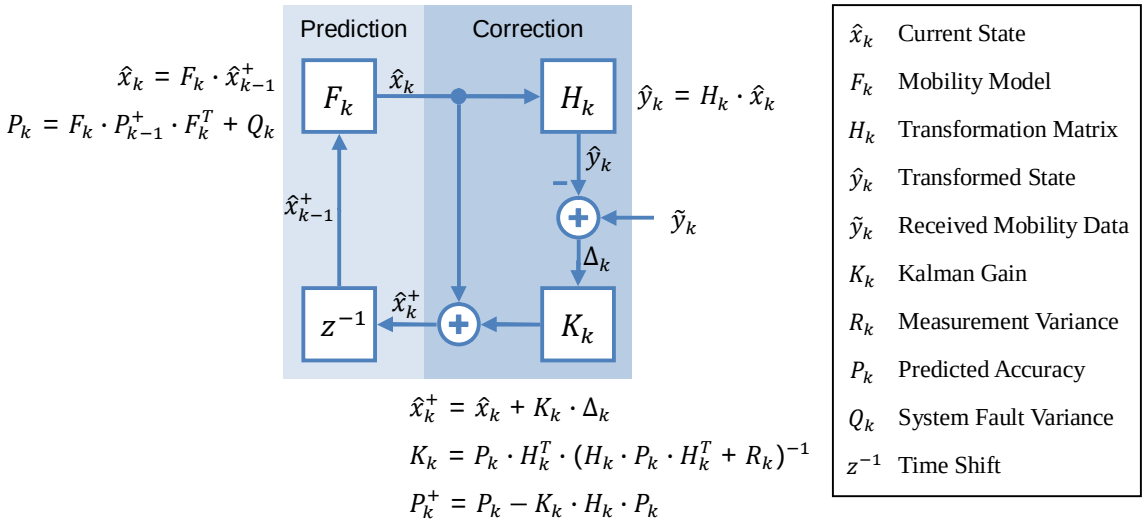

Figure 3: Kalman Filter Schematic and Equations

This Kalman filter is embedded into a framework to deliver vehicle movement prediction used to evaluate mobility data, as presented in the following section.

MOBILITY VERIFICATION FRAMEWORK

As presented in Figure 4, each received C2X message is delivered serially to the mobility verification framework. This message contains mobility data as well as the respective vehicle ID, which may change due to pseudonym changes.

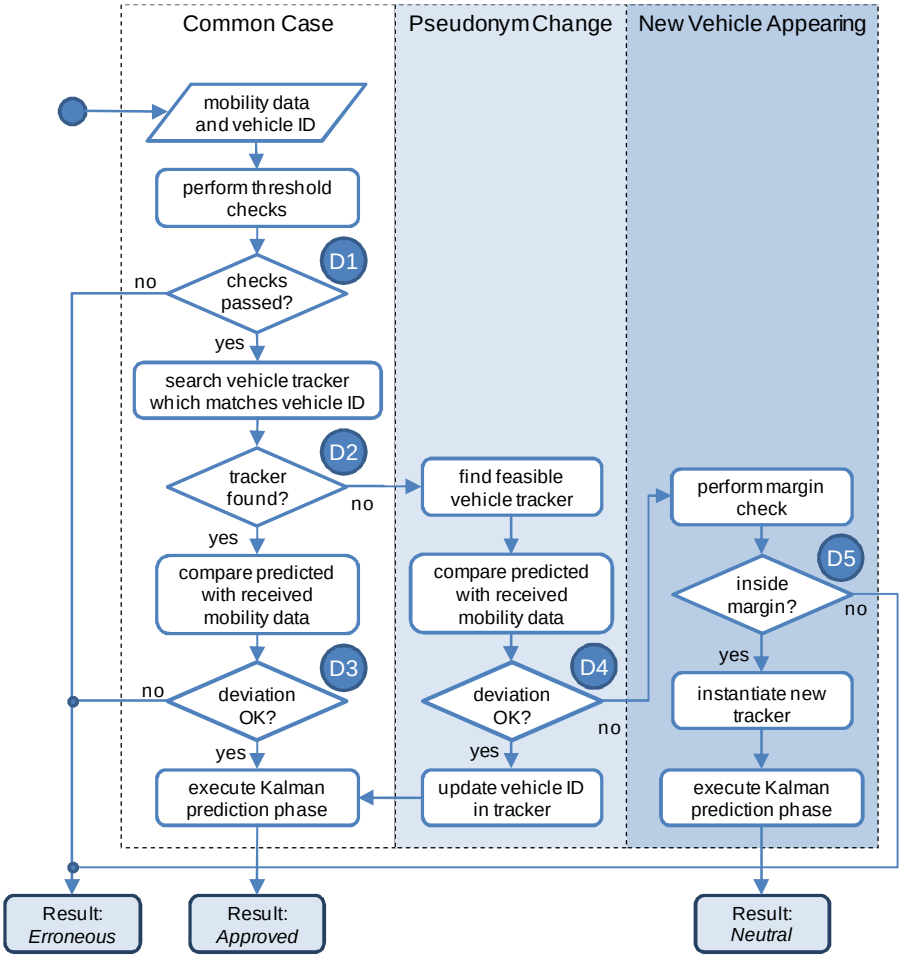

Figure 4: Flow Chart of the Mobility Verification Framework

The first step of the mobility verification contains several threshold checks. Thereby the following values are checked to be inside pre-defined boundaries.

- Velocity as proposed in [8]. This check considers maximum velocities with respect to urban, rural, and motorway scenarios.
- Frequency of incoming CAM messages originated from the same vehicle. This check is based on the maximum beacon interval of 100 ms [13] as proposed in [3].
- Position of the sending vehicle. The vehicle position of the sender has to be inside the communication range of the receiving vehicle. The maximum acceptance range threshold, as proposed in [8], is depicted in Figure 5 as r_{max}.
- Timestamp as proposed in [11]. Expired timestamps or timestamps which are dated to a future point in time are regarded as untrustworthy.

A message will be evaluated as *Erroneous*, if one of the above threshold checks fails (D1). Otherwise, the provided vehicle ID is used to select the appropriate vehicle tracker. For the most common case, vehicles inside the communication range are assumed to be known. Hence, a tracker may be found (D2). The assigned tracker is used to compare received mobility data with the deployed mobility model. For this purpose, the Kalman filter correction phase is triggered with received mobility data $\tilde{y}_k$. The thereby calculated difference Δ_k

considering Kalman Gain K_k gives evidence on trustworthiness of the message. Thus, it may be evaluated as *Erroneous* or *Approved* (D3). Finally, to reduce evaluation delay for upcoming messages, the prediction phase of the Kalman filter is executed in advance.

In case that no vehicle tracker was found (D2), a vehicle within the communication range may have changed its pseudonym. In order to make the pseudonym change transparent, the mobility verification framework searches for an appropriate vehicle tracker by comparing the received and predicted mobility data of all existing trackers. The most feasible tracker is chosen. If vehicle movement fits the prediction of this tracker, then the message is evaluated as *Approved* and a pseudonym change is considered to be detected. Consequently, the associated vehicle ID is updated and the next prediction phase is performed.

If no correlation with the prediction is detected, a margin check indicates whether a new vehicle enters the communication range. The principle of this check refers to sudden appearance warning as proposed by [3]. As depicted in Figure 5, we assume a maximum distance d_{margin}, in which a vehicle may drive inside communication range r_{max} of *vehicle A* without *vehicle A* having received a message. Consequently, a message indicating a vehicle appearing within $r_{max} - d_{margin}$ is marked as *Erroneous*. Due to high message lost in urban scenarios, wider margin dimensions have to be chosen.

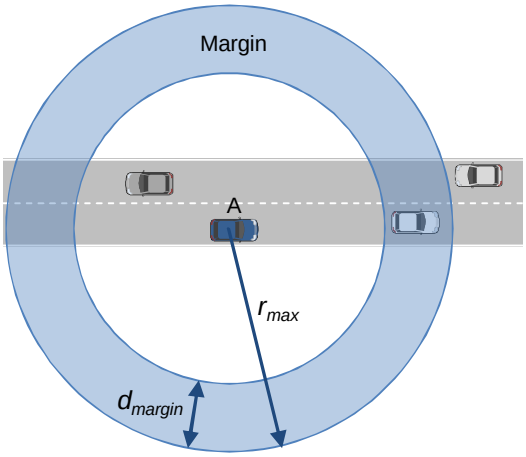

Figure 5: Acceptance Margin Range for Appearing Vehicles

Only in case that a message indicates a vehicle appearing within the margin, a new vehicle tracker will be generated with the provided mobility data. For this new vehicle, the mobility verification framework cannot make any statement on trustworthiness of vehicle mobility. Therefore, the message is evaluated as *Neutral*.

The possible results of the mobility verification framework are summarized in Table 1. Three validation classes are provided, that can easily be interpreted and used by applications on the corresponding vehicle.

Table 1: Message Validation Classes

Validation Class	Description	Recommendation
Erroneous	The mobility data does not match the mobility model of the verification framework.	Message has to be discarded.
Neutral	The framework cannot make a reliable and meaningful statement.	Additional checks on application layer are necessary.
Approved	Mobility data of the message was checked and accepted.	Message can be used by an application.

IV. INTEGRATION INTO THE SIM^{TD}-ARCHITECTURE

According to [14] the sim^{TD} vehicle station is composed of two separated units: a *Control Communication Unit* (CCU), using a 400 MHz automotive PC, and an *Application Unit* (AU), using a 1 GHz automotive PC. Both parts are interconnected via Fast Ethernet. The CCU integrates all components to process C2X communication up to network layer, cryptographic operations as well as pseudonym change management. The AU hosts all sim^{TD} applications and components for basic services, e.g., navigation, human machine interface (HMI), and a message container. While CCU components are developed in C/C++, the majority of AU components, including the mobility verification framework, are realized as Java-OSGi bundle[3].

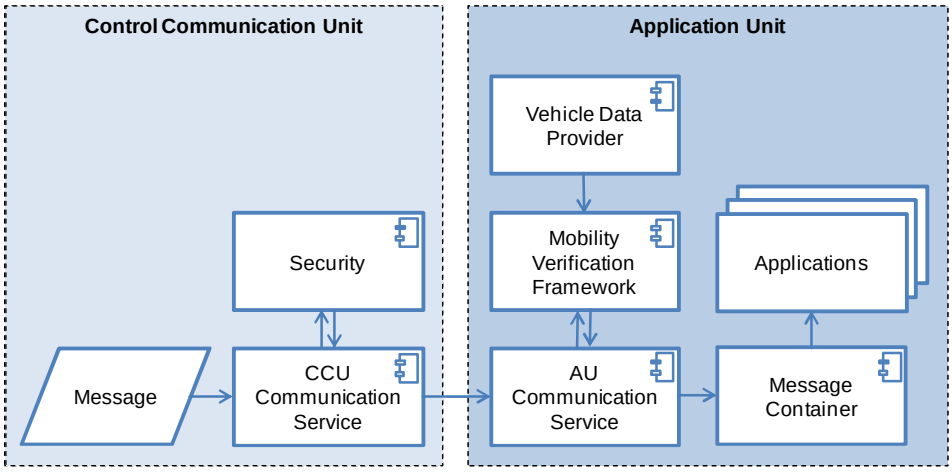

Figure 6: Integration of Mobility Verification Framework into sim^{TD}-Architecture[4]

As shown in Figure 6, every incoming message is parsed by the CCU before being delivered to the AU communication service. Since all sim^{TD} messages are signed digitally by the sending CCU, only messages are processed whose signature was successfully verified by the

[3] See respective OSGi alliance website: http://www.osgi.org

[4] For reasons of clarity the sim^{TD} architecture has been reduced to involved components.

security component. In order to perform mobility checks on the message, the mobility verification framework has access to own mobility information such as position, velocity, heading, and local time provided by a vehicle data provider. Vehicle data is gathered from the vehicle CAN (Controller Area Network) and distributed inside the sim^{TD} architecture. The framework evaluates the message before it is injected into the message container. All components and applications on the AU access the received messages including the verification result via the message container.

To predict future vehicle movements by the mobility verification framework, a Kalman filter-based tracker is instantiated for every adjacent vehicle and updated every time a message is mapped to it. If there is no message assigned to a tracker for a given time, a tracker management removes this tracker to release memory and save processing time.

Since the final sim^{TD} C2X communication unit is not yet available, the mobility verification framework could not be tested on its target platform. Nevertheless, the evaluation delay of the framework is measured on a comparable platform with equivalent processing unit and memory, using C2X messages with simulated vehicle mobility data.

For all three branches of the verification framework, as depicted in Figure 4, simulations have been performed with respect to two different vehicle densities. We notice that for an average density of 10 vehicles in the communication range the overall delay is negligibly low. Even for a maximum load of 100 vehicles, similar performances rates of approximately 1ms were achieved. The Kalman filter prediction has been refined to an average accuracy of about 3 m. The memory consumption does not exceed 1 Megabyte.

Table 2: Maximum Message Evaluation Delay for Two Different Vehicle Densities

Framework Verification Branch	10 vehicles	100 vehicles
Common Case	1.013 ms	1.023 ms
Pseudonym Change	1.201 ms	1.224 ms
New Vehicle Appearing	1.212 ms	1.231 ms

V. CONCLUSION AND FUTURE WORK

In the context of security architecture development of sim^{TD}, a novel framework for mobility data verification was presented. This framework puts already published verification techniques [8][3] into practice and introduces as a novel method a Kalman filter-based approach for reliable mobility data verification. To overcome difficulties due to changing pseudonyms, we applied a tracking algorithm approach, which assigns each vehicle a

permanent identifier. As this identifier together with the vehicle ID never leaves the vehicle AU, privacy is preserved. While being a valid assumption for field operational tests, this may not be the case in later deployment scenarios. Consequently, the tracking operation has to be performed on tamper proof devices, denying access to possible adversaries.

All presented concepts have been implemented as Java-OSGi bundles and are integrated into the overall sim^{TD} vehicle architecture. Simulations have been carried out to prove the technical feasibility of our approach. Worst case analysis yielded acceptable performance rates.

In our future work, we will adapt and further refine our concept by means of real-world measurements obtained from the sim^{TD} field trial. An essential question to be answered by the field trial is related to the packet loss rate, i.e., how many messages might get lost because of shadowing? Especially for urban scenarios, this may become a major issue and consequently will require sophisticated verification strategies.
Furthermore, to improve accuracy of the Acceptance Margin Range check, we will investigate more on appropriate techniques to distinguish messages that are sent from vehicles which are turning on the engine form those messages sent by an attacker.

VI. ACKNOWLEDGEMENT

This work was funded within the project sim^{TD} by the German Federal Ministries of Economics and Technology as well as Education and Research, and supported by the German Federal Ministry of Transport, Building, and Urban Development.

REFERENCES

[1] P. Papadimitratos, "On the Road - Reflections on the Security of Vehicular Communication Systems," in *IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, Columbus, USA, 2008.

[2] T. Leinmüller, E. Schoch, and C. Maihöfer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks," in *Conference on Wireless On demand Network Systems and Services (WONS)*, Obergurgl, Austria, 2007.

[3] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle Behavior Analysis to Enhance Security in VANETs," in *Workshop on Vehicle to Vehicle Communications (V2VCOM)*, Eindhoven, the Netherlands, 2008.

[4] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for Secure and Private Vehicular Communications," in *International*

Conference on ITS Telecommunication (ITST), Sophia Antipolis, France, 2007.

[5] N. Bißmeyer, H. Stübing, M. Mattheß, J. P. Stotz, J. Schütte, M. Gerlach, and F. Friederici, "simTD Security Architecture," in *Embedded Security in Cars Conference (escar)*, Düsseldorf, Germany, 2009.

[6] Intelligent Transportation Systems Committee, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," IEEE Vehicular Technology Society Standard 1609.2™-2006, 2006.

[7] J.-P. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles," *IEEE Security & Privacy Magazine*, vol. 2, no. 3, pp. 49-55, May 2004.

[8] T. Leinmüller, E. Schoch, and F. Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks," *IEEE Wireless Communications Magazine, Special Issue on "Inter-Vehicular Communications"*, Oct. 2006.

[9] M. Torrent-Moreno, P. Santi, and H. Hartenstein, "Distributed Fair Transmit Power Adjustment for Vehicular Ad Hoc Networks," in *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Reston, USA, 2006.

[10] CAR 2 CAR Communication Consortium, "C2C-CC Manifesto," CAR 2 CAR Communication Consortium, Report, 2007. [Online]. www.car-to-car.org

[11] T. Leinmüller, R. K. Schmidt, E. Schoch, A. Held, and G. Schäfer, "Modeling Roadside Attacker Behavior in VANETs," in *IEEE Workshop on Automotive Networking and Applications (AutoNet)*, New Orleans, USA, 2008.

[12] S. Cooper and H. Durrant-Whyte, "A Kalman filter model for GPS navigation of land vehicles," in *International Conference on Intelligent Robots and Systems (IROS)*, Munich, Germany, 1994.

[13] ETSI, " „Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications [Part 2: Specification of Cooperative Awareness Basic Service " V1.1.1," ETSI Technical Specification ETSI TS 102 637-2, April 2010.

[14] H. Stuebing, M. Bechler, D. Heussner, T. May, I. Radusch, H. Rechner, and P. Vogel, "simTD: A Car-To-X System Architecture For Field Operational Tests," *IEEE Communications Magazine - Automotive Networking Series*, May 2010.