A Two-Stage Verification Process for Car-to-X Mobility Data based on Path Prediction and Probabilistic Maneuver Recognition

Hagen Stübing
Adam Opel AG
Advanced Active Safety
Rüsselsheim, Germany
Email: hagen.stuebing@de.opel.com

Jonas Firl
Adam Opel AG
Advanced Active Safety
Rüsselsheim, Germany
Email: jonas.firl@de.opel.com

Sorin A. Huss
Technische Universität Darmstadt
Integrated Circuits and Systems Lab
Darmstadt, Germany
Email: huss@iss.tu-darmstadt.de

***Abstract*—Security is a prerequisite for successfully establishing Car-to-X technology on the market. Sender authentication, message integrity as well as plausibility of the message content represent one of the key aspects in this domain. While the first two requirements are covered by means of cryptography, the latter is still subject to current research. Recent works in the area of vehicle behavior analysis include promising approaches, but are still prone to errors in case of highly dynamic driving maneuvers. In this work we present a novel two-stage verification process for reliable Car-to-X mobility data verification. The first stage consists of a mobility estimator realized by a Kalman filter. The Kalman filter is thereby used to evaluate received mobility data with respect to the path history of vehicles. In the second stage a plausibility check for highly dynamic traffic situations is applied using probabilistic traffic maneuver recognition based on Hidden Markov Models. The overall framework is implemented and its effectiveness is evaluated by means of real world experiments.**

***Index Terms*—Car-to-X Communication, Security, Mobility Data Verfication, Maneuver Recognition, Hidden Markov Model**

I. Introduction

Car-to-X (C2X) communication in terms of Car-to-Car (C2C) and Car-to-Infrastructure (C2I) communication aims to increase road safety and traffic efficiency by exchanging foresighted traffic information. C2X applications thereby range from road safety and traffic efficiency to service-oriented applications. Since the initial earmarking of 802.11p frequencies [1] by the European Commission in 2008, vehicular communication networks have made through a great progress. Based on the message set as currently standardized by ETSI, several field operation tests like DriveC2X [2] and sim^{TD} [3] are being conducted. Cooperative Awareness Messages (CAMs) include a vehicle's mobility data in terms of position, speed, and heading and are sent within intervals from 1s to 100 ms [4]. In contrary, Decentralized Notification Messages (DENMs) are sent only upon detection of certain traffic events, like, e.g., black ice or traffic jams, and may be forwarded over longer distances. The ETSI furthermore has identified security and privacy issues as a key-enabler for C2X and therefore has settled it a cross-layer among all other ITS layers [5]. Consequently, the Car-to-Car Communication Consortium has developed a first proposal for a Public Key Infrastructure (PKI) [6], which provides digital certificates and signatures to authenticate the trustworthiness of C2X messages. This PKI deploys the standard IEEE 1609.2 [7] and is currently included into further standardization activities within ETSI WG 5.

However, securing inter-vehicular communication by means of cryptography represents a necessary, though not fully sufficient countermeasure against forging of messages. Any adversary, who has gained access to secrete key material stored within the C2X module, will still be able to send authenticated messages. Such an attacker cannot be detected by means of cryptography only and consequently requires complementary security techniques based on behaviour analysis.

In this work a novel two-stage verification process for Car-to-X mobility data is proposed. The first stage consists of a Kalman filter as a means of detecting the continuum of motion as a verification criterion. This Kalman filter based verification approach is currently deployed within field operational trials like sim^{TD} [8]. While being an effective and reliable estimator in most traffic scenarios, we identified considerable issues in cases of highly dynamic traffic scenarios like, e.g. suddenly overtaking or hard braking vehicles. In consequence, trustworthy messages may be evaluated as non-plausible which will result into an decreased safety level of the overall C2X system. Since lowering the security thershold for message acceptance is not an option for us, we investigate in complementary techniques for increasing reliability by means of maneuver recognition algorithms. Hence, we propose to include a second stage of C2X mobility verification and calibrate our Kalman filter based model accordingly.

This paper is structured as follows: After this introduction we present the underlying attacker model in section II and thereby motivate the necessity for mobility data verification in C2X networks. In section III we discuss related work in the area of C2X message verification. The proposed two stage verification process is detailed in section IV. We first present each verificaiton stage individually and then describe how the overall framework is constituted. In section V we carry out ex-

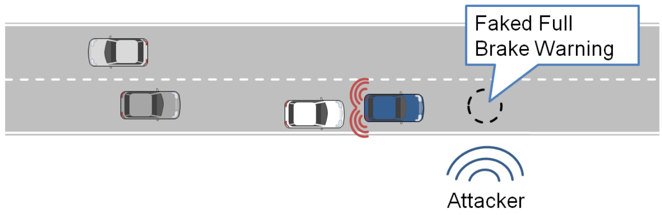


Fig. 1. Faked full brake warning

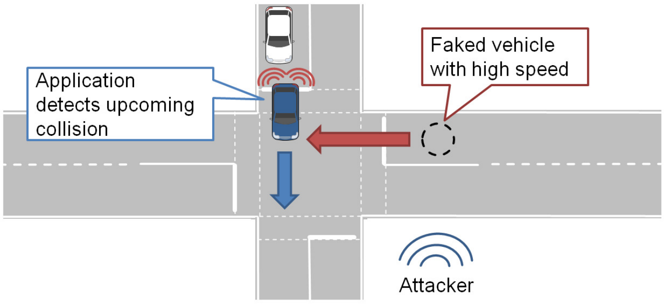


Fig. 2. Faked intersection collision warning

periments and evaluate the effectivness of this novel approach. Finally, in sectionVI we summarize our contributions and give some remarks on future work.

II. Attacker Model

In this work we assume a severe adversary, which has gained access to a vehicles internal network (GPS, CAN, etc.), and is therefore able to manipulate the information sent to the C2X module. Depending on the adversary's intentions, several attack scenarios are imaginable:
For instance, in Figure 1 an attack on the Emergency Brake Light (EBL) use case is illustrated. We assume a roadside attacker, which is equipped with a common C2X module, including valid security credentials. By simulating a full brake to the C2X module, the respective warning message is created. If the adversary has also capabilities for manipulating the internal GPS interface, any reference position can be introduced. Since the final message will be signed using valid keys, those faked messages cannot be detected on the receiver side by means of cryptography. Hence, the driver will be alerted of a sudden full brake in front of him. As we expect drivers to instantly react upon warnings, such a situation may lead to unexpectedly performed collision mitigation maneuvers.
A similar scenario is depicted in Figure 2. The Intersection Collision Warning (ICW) according to [9] is a use case, where vehicles are monitoring cross traffic when entering an intersection in order to detect possible upcoming accidents. In the illustrated scenario a static roadside attacker is sending a faked CAM, indicating a vehicle approaching the intersection with a very high speed. The application running on vehicle A's C2X module detects a potential hazard and notifies the driver accordingly. In principle the previously described scenarios may also be caused by inaccurate readings from the GPS receiver or malfunctioning of the C2X sender hardware. We argue that for message evaluation on the receiver no distinction between these two cases is made.

III. Related Work

In order to motivate the necessity of position verification approaches in [10] the influence of falsified position data on geographic routing is analyzed. A significant reduction of successfully delivered messages depending on the network size and the percentage of malicious nodes is observed. As a countermeasure the authors propose a combination of both, autonomous as well as cooperative verification approaches. Observations obtained from every verification sensor are weighted according to their reliability and then combined into an overall trust value for the respective neighboring vehicle. Some of the suggested autonomous checks, like, e.g., ART and MGT, are also included into the proposed framework in this work.
In [11] the checks proposed by [10] are included into an overall evaluation scheme called VEBAS (VEhicle Behavior Analysis and Evaluation Scheme). Besides already known checks, further modules are introduced to detect suddenly appearing vehicles or irregularities within the sent beacon message frequency. In [12] the authors go further into detail with the module called Minimum Distance Moved (MDM). Assuming that attacks are likely to be launched by a stationary roadside attacker, the MDM module constantly assesses the trajectory of neighboring vehicles. Since the communication range of a stationary attacker is limited, any sender, which is still received by the host vehicle after a certain time, cannot be a roadside attacker and consequently will be assigned a higher trust value. In VEBAS the different assessments are grouped into checks which are confirming and those which are rejecting a given position claim, respectively. Outputs of different modules are averaged over time and assigned to an aging function in order to reflect the influence of past ratings on the current evaluation. In order to increase reliability of evaluations, [11] also suggests to share recommendations between vehicles in a cooperative manner. For instance, in [13] the results of the aforementioned MDM test are proposed to be exchanged among neighbors in order to shorten the evaluation time and to cope with attackers, which are increasing their communication range above common thresholds.
While previous approaches are based on information obtained from received C2X messages only, the authors in [14] focus on techniques based on cross verification via a vehicles on-board radar sensor. Assuming that every vehicle taking part in the C2X communication network is also equipped with 360 degree radar, a fusion between both information sources is performed, taking into account the specific inaccuracies of each technology.

IV. Two-Stage Mobility Verification Framework

The proposed framework consists of a two-stage verification process. Accordingly, the first part of the evaluation is related to the comparison between received and predicted mobility data by means of a given mobility model as introduced in [8].

However, due to unavoidable inconsistencies of the deployed system model, the underlying Kalman prediction contains errors. In order to achieve a higher reliability for the overall system, additional measures based on maneuver recognition via Hidden Markov Models are proposed. In the following we give a brief introduction into the basic theories of Kalman filter and Hidden Markov Model, respectively. Then, we describe how these concepts are exploited and deployed for the purpose of vehicle tracking.

A. Path Prediction

In this section we outline the basic concept and implementation of the first evaluation stage which consists of a Kalman filter for predicting and evaluating the mobility data of adjacent vehicles.

1) Kalman Filter: The Kalman filter (KF) method as denoted by the equations originally published in [15] represents a well-known and effective approach to multi target tracking. It intends to minimize the mean squared estimation error of a system state, taking into account noise of the measurement data as well as uncertainties of the underlying system model. Compared to other minimum square methods, the Kalman filter has the clear advantage that it works recursively. Hence, this approach does not require to store and to process the entire set of previously received data for predicting the next estimate. Besides that, the KF is based on time-discrete models and may consider dynamic noise for its calculations. Because of these properties, this method is particularly well-suited for the purpose of estimating future vehicle states based on C2X messages.

For every received measurement sample, received at time step k, the KF executes two successive phases, i.e., prediction and update. The KF approach to predict the next state requires some apriori information on the system itself. This knowledge is modeled by the *state transition matrix* F_k. Hence, to predict the next *system state* $\hat{x}_k$ based on the *current state* $\hat{x}_{k-1}^+$, the following state space equation is applied:

$$\hat{x}_k = F_k \cdot \hat{x}_{k-1}^+ \tag{1}$$

Furthermore, during this phase also an estimate on the inaccuracies related to the current prediction is calculated. These inaccuracies are mainly due to unavoidable uncertainties within the system model. Accordingly, the prior *prediction error covariance* P_k is calculated recursively by accumulating the *previous prediction error* P_{k-1}^+ (taking into account the transition matrix F_k) to the *system noise* Q_k:

$$P_k = F_k \cdot P_{k-1}^+ \cdot F_k + Q_k \tag{2}$$

For every time step k, the prediction phase is followed by an update phase, which consists of a correction of the predicted state by means of the *sampled data* $\tilde{y}_k$ observed from the system. For that purpose, the *distance* Δy_k between sampled data $\tilde{y}_k$ and predicted data $\hat{x}_k$ is determined, using transition matrix H_k, which reflects the correspondence between system state and measurement.

$$\Delta y_k = y_k - H_k \cdot \hat{x}_k \tag{3}$$

A significant part within the KF is related to the calculation of the Kalman gain:

$$K_k = P_k \cdot H_k^T \cdot (H_k \cdot P_k \cdot H_k^T + R_k)^{-1} \tag{4}$$

The *Kalman gain* K_k represents a measure for balancing predicted and measured data taking into account both the system noise (accumulated in P_k) and the noise contained in the measurement itself (denoted as *measurement variance* R_k). Note that system and measurement noise are assumed to be statistically independent. Accordingly, the corrected system state $\hat{x}_k^+$ is calculated as:

$$x_k^+ = \hat{x}_k + K_k \cdot \Delta y_k \tag{5}$$

As a final step, the prediction error covariance matrix P_k is updated by means of the Kalman gain:

$$P_k^+ = P_k - K_k \cdot H_k \cdot P_k \tag{6}$$

2) Kalman Filter for Vehicle Path Prediction: The KF method is widely used in the automotive domain for applications like, e.g., navigation. There, a technique called dead reckoning [16] is applied, which intends to overcome the reduced quality of GPS signals by taking into account the vehicles local data, such as, e.g., yaw rate and steering angle. This application is well comparable to our scenario, even though the state parameters might be different. For the purpose of vehicle tracking, the related matrices are defined as follows. We denote the system state in terms of the vehicles mobility data represented in Cartesian coordinates. Hence, a vehicles position (p_x, p_y) and velocity (v_x, v_y) are components of a vector of the form:

$$\hat{x}_k = \begin{pmatrix} p_x \\ p_y \\ v_x \\ v_y \end{pmatrix} \tag{7}$$

The accuracy of the system model is limited by the entropy of the data of received C2X messages. Since, in the present version of CAM implementation, only position, speed, and heading are transmitted, we build our system model under the assumption of constant velocity. Consequently, the previous system state will be transferred to the next state according to the physical laws of motion by applying the following matrix.

$$F_k = \begin{pmatrix} 1 & 0 & \Delta t_k & 0 \\ 0 & 1 & 0 & \Delta t_k \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{8}$$

For calculating the prediction error covariance matrix P_k we have to elaborate the error related to the system model in (8). This tuning process is generally referred as system identification and is performed offline with the help of several reference traces. We observed slightly deviant behaviors for different road scenarios, i.e., motorways, rural or city roads.

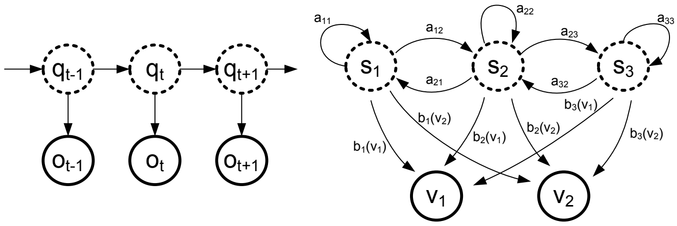


Fig. 3. Structure of a HMM. Left: Markov chain of hidden system states. Right: HMM with 3 system states and 2 (discrete) observation symbols v_1 and v_2.

Although currently not yet implemented in our framework, we recommend a dynamic switching of the applied system noise matrix Q_k for an enhanced evaluation. In contrast, the measurement variances R_k need not to be evaluated, since every mobility data transmitted via CAMs also includes additional values with respect to the specific accuracy.

B. Probabilistic Maneuver Recognition

An essential part of the proposed mobility verification process consists of the second stage, which is related to the recognition of traffic maneuvers. Using this information a more accurate assessement of the current traffic situation can be performed. In this work we advocate a probabilisitc maneuver recognition approach based on Hidden Markov Models, which is described in the following.

1) Hidden Markov Model: A Hidden Markov Model (HMM) is a probabilistic method to model dynamic systems with unknown (hidden) states. It is defined by (see [17]):

- A set of (hidden) system states $X = (X_1, \dots, X_N)$, where the sequence of hidden states $\vec{q} = (q_t)_{t=1,\dots,T}$ is a Markov chain: $P(q_t|q_{t-1}, \dots, q_1) = P(q_t|q_{t-1})$. The state transition probabilities are collected in the matrix $A = \{a_{i,j}\}$ with

$$a_{i,j} := P(q_{t+1} = X_j | q_t = X_i).$$

- The observation probabilities

$$b_j(o) := P(o|X_j)$$

  of an observation o while being in state X_j are collected in the matrix B. Due to continuous observations, the observation is usually parametrized by using Mixtures of Gaussians (MoG).
- The probability of being in state X_i at the beginning of the state sequence is

$$\pi_i := P(q_1 = X_i).$$

Therefore, a HMM can be denoted by $\lambda = (A, B, \pi)$. The general structure of a HMM is illustrated in Figure 3. One of the main advantages of using this approach for modeling sequential data is the availabilty of highly efficient algorithms for parameter learning and for performing inference.

a) Recognition with HMMs: The recognition problem consists of the computation of the likelihood of an observation sequence $\vec{o} = (o_1, \dots, o_T)$, given a model λ: $P(\vec{o}|\lambda)$. Thus, various models λ_i may be compared with respect to an observation sequence. In general, this problem is solved by computing the likelihood for all possible state sequences $\vec{q}$ of length T:

$$P(\vec{o}|\lambda) = \sum P(\vec{o}, \vec{q}|\lambda).$$

Because there are N^T possible state sequences, this calculation is computationally unfeasible even for small values of N and T. Consequently, a more feasible approach has to be derived. Therefore the *forward variables* are defined as:

$$\alpha_t(i) := P(o_1, \dots, o_t, q_t = X_i|\lambda). \tag{9}$$

By making use of the Markov property of HMMs $\alpha_t(i)$ can be computed by induction:

1) Initialization:

$$\alpha_1(i) = \pi_i b_i(o_1), \quad i = 1, \dots, N \tag{10}$$

2) Induction:

$$\alpha_t(j) \left[\sum_{i=1}^{N} \alpha_{t-1}(i) a_{ij} \right] b_j(o_t), \quad t = 2, \dots, T \tag{11}$$

3) Termination:

$$P(\vec{o}|\lambda) = \sum_{i=1}^{N} \alpha_T(i), \tag{12}$$

and with the last step the required probability is available (see [17] for details).

b) Parameter estimation: Another problem to be solved when applying HMMs is related to the estimation of the model parameters (A, B, π). In general, this problem is solved by maximizing the likelihood of a set of training observations $\vec{o}_{train}$, i.e.:

$$\hat{\lambda} = \underset{\lambda}{\operatorname{argmax}}\, P(\vec{o}_{train}|\lambda). \tag{13}$$

Due to the fact that there does not exist an analytical solution to this problem, iterative approximation procedures like the *Baum-Welch-algorithm* are to be applied (see [17], [18]). Like other iterative algorithms for non-convex problems, the Baum-Welch-algorithm is only able to locally maximize the above likelihood. This is why the algorithm will converge to a local maximum depending on the initial parameters, which have to be chosen appropriately.

2) HMM for maneuver recognition: Hidden Markov Models for recognition of traffic maneuvers were first introduced in [19]. One model λ_i is trained for every maneuver to be classified using the *Baum-Welch-Algorithm*. The states of the model correspond to the different physical stages of the maneuver as depicted in Figure 4). To implement a traffic maneuver recognition based on HMMs, the first step is to define and identify crucial maneuvers, like, e.g., *overtaking*, *following*, and *flanking*.

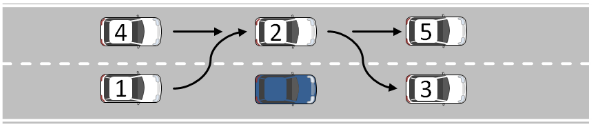


Fig. 4. Different stages of an overtaking maneuver, which correspond to the (hidden) states of the HMM.

The observation data is relational information about two interacting vehicles (e.g., relative position, speed, accelaration) and is integrated using a MoG model. In this work the information of the received mobility data is used to extract the required observation data, i.e., the relative values about position (2-dimensional) and velocity (1-dimensional):

$$o_t = (p_x, p_y, v). \tag{14}$$

Every time a new vehicle enters the communication range of the host car the evaluation process is initiated (see section IV-C).

After that, recognition is done by using *forward algorithm* of every model (see (9) to (12)) for the observation sequence $\vec{o}$ yielding $P(\vec{o}|\lambda_i)$. For more detailed information see [20]. Rewriting this likelihood using the basic equation of the Bayes theory and the assumption of a constant observation probability $P(\vec{o})$

$$P(\lambda_i|\vec{o}) = \frac{P(\vec{o}|\lambda_i) \cdot P(\lambda_i)}{P(\vec{o})} \propto P(\vec{o}|\lambda_i) \cdot P(\lambda_i) \tag{15}$$

results on the one hand in a more meaningful value. On the other hand the a-priori probability $P(\lambda_i)$ can represent the influence of varying road types on different driving maneuvers. For example, an overtaking maneuver is more likely to occur on a highway than on a country road.

The purpose of the maneuver recognition approach as integrated in the verification framework is to make two different high dynamic maneuvers plausible: lane change and braking maneuvers, as depicted in Figure 6.

a) Lane Change Recognition: Most dynamic lane changes (Figure 6a), especially on extra-urban roads, are performed when doing an overtaking maneuver. Lane changes are one of the high dynamic maneuvers, where due to a suddenly occuring lateral offset, the Kalman deviation Δy_k in (3) is exceeding the predefined threshold. The recognition of such situations is subject to two different HMMs: overtaking λ_{over} and following λ_{foll}. With these two models the likelihoods $P(\lambda_i|\vec{o})$ can be computed according to (15). If a maneuver recognition is queried ((D4) in Figure 5) the ratio

$$r = \frac{P(\lambda_{over}|\vec{o})}{P(\lambda_{foll}|\vec{o})}$$

has to be evaluated. High values of r, especially when being in state 1 of Figure 4, correspond to a higher lane change probability. For our purpose we are interested in finding situations where a high deviation Δy_k coincides with a ratio r close to 1. For these cases peaks in Δy_k can be made plausible.

b) Braking Maneuver Recognition: The reason for spontaneous brakings as on bottom of Figure 6b is often the driver's intention to start an overtaking maneuver, but which cannot be initialized due to insufficient free space on the left lane. This means braking maneuvers often occur when driver intention and real maneuver feasibility diverge. This circumstance is not modeled by the observation vector (14). Hence, braking maneuvers cannot be detected by evaluating the likelihoods $P(\vec{o}|\lambda_i)$ as for the previous scenario. Therefore, a second model needs to be trained, where the observation vector takes the free space into account, too:

$$o_t = (p_x, p_y, v, f). \tag{16}$$

The variable $f \in [0, 1]$, influenced by road geometry and other traffic participants, indicates the certainty for enough free space for performing the overtaking maneuver. The detection of braking maneuvers is performed by evaluating the ratio of the likelihoods of the overtaking maneuvers with the adapted observation vector (16) and the basic observation vector (14), respectively.

C. Two-Stage Mobility Data Verification Flow

In Figure 5 the two-stage verification process is illustrated. Similar to the basic scheme presented in [8], the mobility data is evaluated with respect to physical and regulatory boundaries. These threshold checks are necessary in order to prevent inconsistent data to corrupt the ongoing evaluation stages. The list of different checks applied can be found in [8] and includes, e.g., checks for maximum velocity, message freshness, and maximum message frequency. Since these checks are rather lightweighted and designed with appropriated tolerances, we require each of them to be passed successfully to continue verification (D1). The first verification stage consists of path prediction and evaluation by means of the KF approach as presented in section IV-A1. Accordingly, for every vehicle within the communication range, the host car instantiates and maintains a tracker including a Kalman filter. The evaluation flow then proceeds as follows:

For new vehicles appearing within communication range (D2), no sophisticated mobility verification can be applied. However, while driving along the road, new vehicles usually appear first on the border of the current communication range r_{max}. Considering a tolerance margin d_{margin}, we require a new vehicle to appear first within the margin $r_{max} - d_{margin}$ and r_{max}. Note that these tolerance margins have to be adapted for different scenarios (e.g., in city scenarios, where starting vehicles may suddenly appear nearby the host vehicle). For higher reliability of the evaluation it is strongly recommended to apply complementary checks based on a vehicle's local sensors as proposed in [21].

For an already known vehicle ID (D2), the assigned vehicle tracker is selected and based on the given timestamp the Kalman prediction phase is triggered. According to equation (2) the difference Δy_k between predicted state $\hat{x}_k$ and received mobility data $\tilde{y}_k$ is determined. Considering a maximum tolerable difference, the trustworthiness of the message is

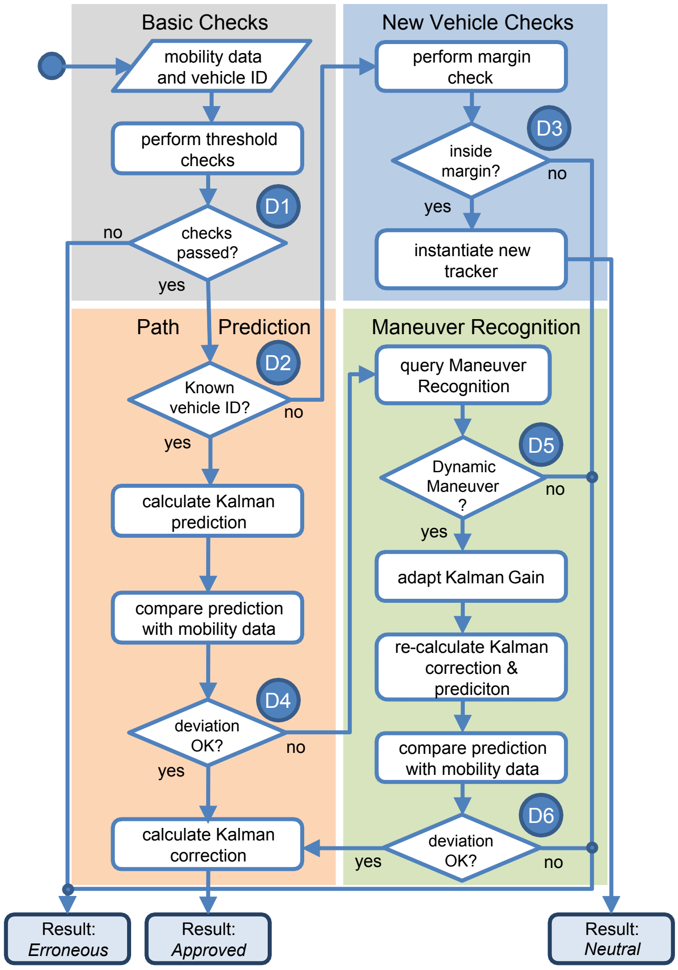
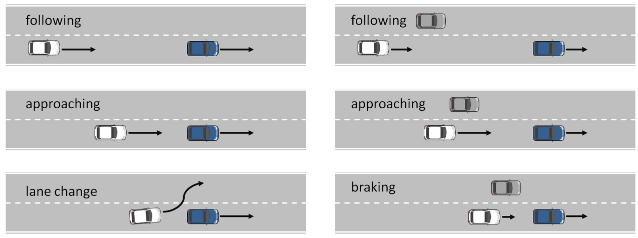


Fig. 5. Verification Flow of mobility data in C2X Communication using Path Prediciton and probabilisitc Maneuver Recognition.

assessed.

The predefined threshold value is established based on common GPS errors, which are typically in the range of $1-3$ meters. In [8] evaluations have been carried out, which yielded acceptable performance margins for most traffic situation. However, due to inherent system inaccuracies, we observed much greater deviations in high dynamic scenarios. To avoid incorrect assessment of messages in such situations, we apply further measures based on maneuver recognition in case that the deviation between predicted and received mobility data is too large (D4). The maneuver recognition component as described in section IV-B permanently assesses traffic situations of vehicles in the communication range and directly provides an estimate to the framework. The current implementation, as described in section IV-B2, is capable of predicting two dynamic maneuvers, i.e., a suddenly overtaking or hard braking vehicles. In case the evaluated message is originated from a vehicle, which is currently performing such a maneuver, we know from experiments that the applied Kalman model reacts too slow on sudden changes of the vehicles trajectory and consequently has to be recalibrated. As already identified in



(a) Lane change maneuver (b) Braking maneuver

Fig. 6. Two use cases for the verification framework.

section IV-A1, the Kalman gain represents the determining factor for weighting the predicted state against the measured data. Accordingly, in such highly dynamic maneuvers (D5), our evaluation framework is adjusting the gain in a way that the state x_k^+ in equation (5) is corrected towards the measurement. For doing so, the previous prediction and correction phase are reversed and recalculated again. Considering an adapted Kalman model, the recalculation leads to an enhanced corrected state, which will directly result into a prediction, which is expected to be closer to the next received mobility data. The deviation is calculated again and if the threshold is passed by now (D5), the message is marked as approved and the respective correction is performed. In contrary, if the deviation still exceeds the predefined threshold, the message is definitely evaluated as erroneous.

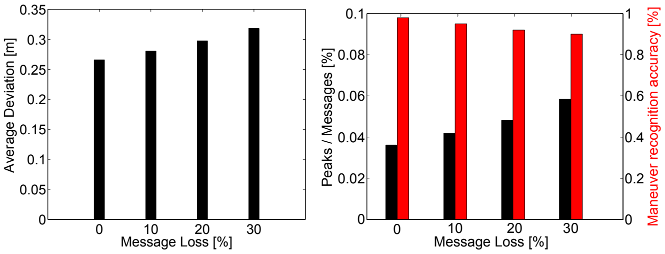
V. Experimental Results

In this section experimental results, when using the verification framework described in the last section, are presented. We use sim$^{\mathrm{TD}}$-equipped vehicles to evaluate the overall system performance in crucial, high dynamic driving situations. The evalutation database consists of approximately 30 overtaking maneuvers and 20 braking maneuvers. In Figure 6 the different stages of the two maneuvers are illustrated. At the beginning both vehicles drive with constant speed (following). Then one vehicle accelerates and approaches the other. In the last stage of the situations an abrupt lane change or braking maneuver is performed. The results of the verification process with and without the maneuver recognition for both of the selected situations will be presented in V-A and V-B.

The maneuver recognition has to distinguish between two different cases:

- The message was marked as incorrect while being in a highly dynamic driving maneuver. In this case the maneuver recognition shall plausibilize the message.
- The message was marked as incorrect while not being in a highly dynamic driving maneuver (e.g., caused by an attacker). In this case the maneuver recognition shall not plausibilize the message.

In order to verify the robustness of the proposed framework, we evaluate its capability to work correctely even in the presence of message losses. In Figure 7a the average Kalman deviation is depicted for different percentages of message losses. For prediction accuracy, it is important which messages



(a) (b)

Fig. 7. (a) Average Kalman deviation for different message losses; (b) Average ratio of peaks to messages compared to accuracy of maneuver recognition for different message losses

are getting lost, so we averaged our results over 1000 different probes. We observed a significant dependancy of the Kalman prediction accuracy on the number of correctly received messages, i.e., the more messages are getting lost, the higher the prediction error becomes.

According to the graphs depicted in Figure 7b the relative occurance of peaks (i.e., messages where the Kalman deviation is above a fixed threshold compared to the total number of received messages) is also increasing for higher message losses. In contrary, the HMM based maneuver recognition prooves high accuracy (above 90%) despite the reduced number of messages. This property is highly beneficial for our purpose of mobility data verification and makes this approach applicable for many communication domains even beyond C2C.

A. Lane Change Maneuvers

The results for the lane change maneuver recognition are shown in Figure 8, where exemplarily one sequence is considered for illustration purposes. As expected, the deviation Δy_k (top of figure) has its peaks during the last stage of the maneuver (messages $37 - 52$). Note that for the current implementation the deviation threshold is set to 1 meter.
The results for the maneuver recognition are shown in the middle part of the figure, where already at the first peak of Δy_k (at message 37) the lane change can clearly be predicted. Note that the reasons for plotting the likelihoods logarithmically are rather small result values from HMM evaluation algorithms. At this time the maneuver recognition is querried the first time (compare to (D4), in Figure 5) because Δy_k is exceeding the given threshold. We observe that during the lane change maneuver the threshold is exceeded up to four times. During this period the maneuver recognition component identifies the lane change correctly.
At the bottom of Figure 8 the deviation $\Delta y_{k,new}$, when deploying the advocated two-stage verification framework, is plotted. As a result of the adapted Kalman gain all peaks of Δy_k are decreased below the given threshold, such that no messages are wrongly marked as erroneous anymore.

B. Braking Maneuvers

The results for the braking maneuver recognition are shown in Figure 9. In order to excercise the procedure described

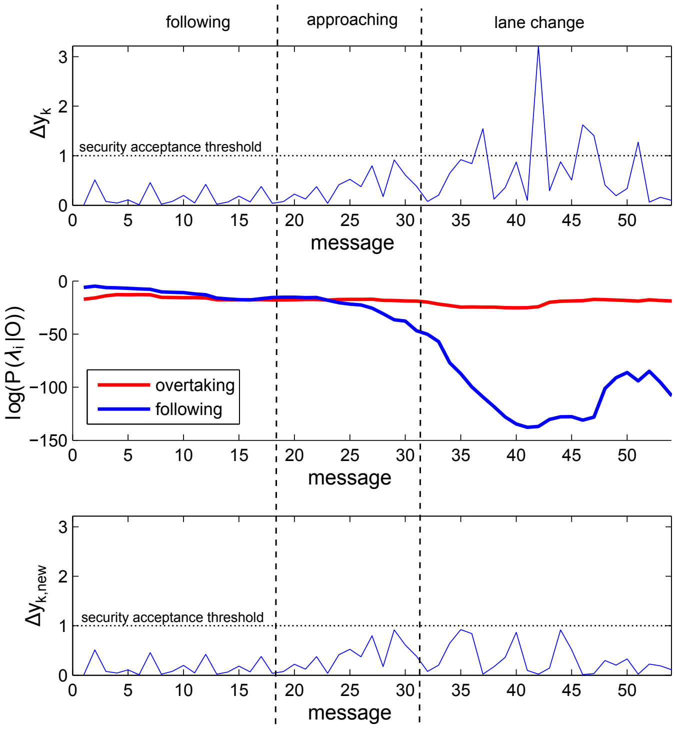


Fig. 8. Lane change maneuver - Top: Kalman deviation Δy_k - Middle: log-likelihood of maneuver recognition - Bottom: Kalman deviation $\Delta y_{k,new}$ with adapted Kalman gain

in paragraph IV-B2 the free space variable f is adapted by modeling a vehicle driving on the left lane (see Figure 6b). At the top of Figure 9 the Kalman deviation Δy_k is plotted again, where the peak appears in the last stage of the sequence, where the vehicle is suddenly braking (message 70) and the maneuver recognition is querried. At this time the driver's intension (overtaking, no free space consideration) is clearly above the real maneuver feasibility (overtaking free space). At the bottom of Figure 9 the corrected deviation $\Delta y_{k,new}$ is plotted, where both peaks of Δy_k were decreased well below the threshold by means of our proposed framework.

VI. Conclusion and Future Work

Precise and trustworthy position data represents a prequisite for successfully deploying the Car-to-X communication technology. Because of its high relvance to most C2X applications, postion informations inside every C2X message is a very attractive target for possible adversaries. There exists a common understanding by C2X security designers that due to limited invehicle security measures, cryptographic solutions will have to be complemented by additional mobility verifications. In this work we reviewed the sim^{TD} mobility verification framework and evalutated its effectiveness for dynamic overtaking and for hard braking maneuvers. Several trial runs with fully equipped sim^{TD} vehicles revealed a considerable mismachting between predicted and actual mobility data for highly dynamic scenarios. These inaccuriacies, if not handeled appropriatly, may lead to an incorrect

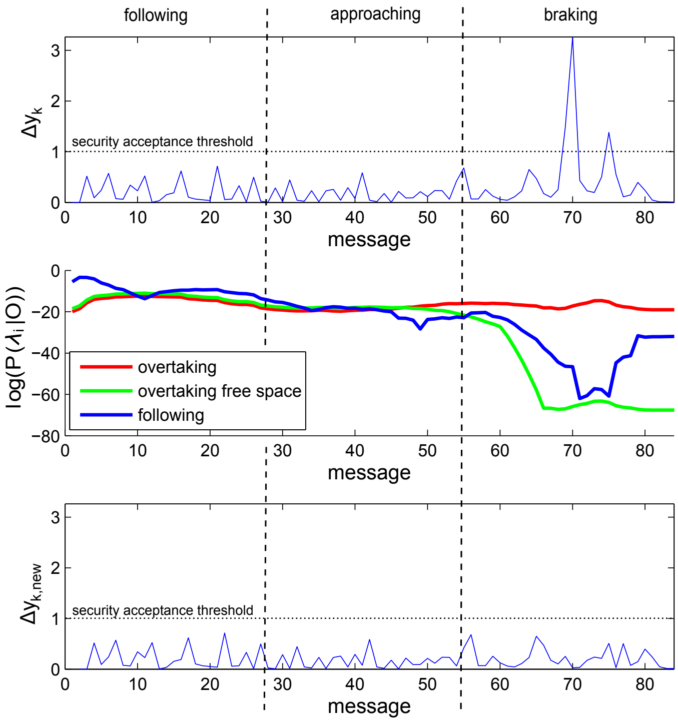


Fig. 9. Braking maneuver - Top: Kalman deviation Δy_k - Middle: log-likelihood of maneuver recognition - Bottom: Kalman deviation $\Delta y_{k,new}$ with adapted Kalman gain

message evaluation. Consequently, the verification framework has to be extended by additional measures. By evaluating the measured data obtained from the performed trial runs, we identified the Kalman gain as the determining factor for influencing the inertia of the applied predicion model. We proposed probabilistic maneuver recognition based on Hidden Markov Models as the control medium for Kalman gain. We carried out several experiments under varying message loss rates, which confirmed the general appropriateness of HMMs for C2X scenarios. An comprehensive two-stage verification framework for mobility data was proposed, which describes how the Kalman verification stage is calibrated by means of a second HMM stage. An implementation of the refined framework and the re-run of previous experiments, yielded significanlty improved accuracies of the prediction model. We conclude that current verification approaches for C2X represent a promising attempt to increase overall security level of the system. However, to make these approaches even more effective, a combination of various sensors, like ,e.g., the presented maneuver recognition, is strongly recommended.

In our future work we plan to further extend the proposed framework by additional information sources. Up to now only frequently sent CAM messages have been taken into account. To increase the reliability of the maneuver recogntion algorithm further information can be extracted from event based messages like the DENM. For instance, a message, which indicates a lane narrowing due to a construction zone, may limit the probability for certain maneuvers on that road section. These and other information may be combined in every vehicle to build up an internal model of the traffic environment and to evaluate new incoming message with respect to that model.

ACKNOWLEDGMENT

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 Federal Ministry of Transport, Building and Urban Development.

REFERENCES

[1] *Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of intelligent transport systems operating in the 5 GHz frequency band*, ITS WG4 Std. ES 202 663, Rev. Ver. 1.1.0, 2010.

[2] "Drive C2X Accelerate Cooperative Mobility," 2011. [Online]. Available: http://www.drive-c2x.eu/project

[3] "simTD: Sichere Intelligente Mobilität Testfeld Deutschland," 2011. [Online]. Available: www.simtd.de

[4] *Intelligent Transport Systems (ITS), Vehicular Communications (VC), Basic Set of Applications, Definitions*, European Telecommunications Standards Institute ETSI Technical Specification TS 102 637-2, April 2010.

[5] *Intelligent Transport Systems (ITS); Communications; Architecture*, European Telecommunications Standards Institute ETSI Technical Specification TS 102 665, 2009.

[6] N. Bißmeyer, H. Stübing, E. Schoch, S. Götz, J. P. Stotz, and B. Lonc, "A generic Public Key Infrastructure for securing Car-to-X Communication (accepted for publication)," in *18th ITS World Congress*, 2011.

[7] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, Intelligent Transportation Systems Committee Std. 1609.2-2006, 2006.

[8] H. Stuebing, A. Jaeger, N. Bissmeyer, C. Schmidt, and S. A. Huss, "Verifying Mobility Data under Privacy Considerations in Car-to-X Communication," in *17th ITS World Congress*, Oct. 2010.

[9] Car to Car Communication Consortium. (2007, August) Car 2 Car Communication Consortium Manifesto. [Online]. Available: www.car-to-car.org

[10] T. Leinmüller, E. Schoch, and F. Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks," *IEEE Wireless Communications, Special Issue on "Inter-Vehicular Communications"*, vol. 13, no. 5, pp. 16–21, Oct. 2006.

[11] R. K. Schmidt, T. Leinmueller, E. Schoch, A. Held, and G. Schaefer, "Vehicle Behavior Analysis to Enhance Security in VANETs," in *Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008)*, 2008.

[12] R. Schmidt, T. Leinmüller, and A. Held, "Defending Against Roadside Attackers," in *In proceedings of 16th World Congress on Intelligent Transport Systems*, 2009.

[13] 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.

[14] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Journal of Computer Communications*, vol. 31, pp. 2883–2897, July 2008.

[15] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal Of Basic Engineering*, vol. 82, no. Series D, pp. 35–45, 1960.

[16] *A Kalman filter for integrating dead reckoning, map matching and GPS positioning*, Aug. 2002.

[17] L. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *Proceedings of the IEEE*, vol. 77, no. 2, pp. 257–286, Feb 1989.

[18] J. Bilmes, "A gentle tutorial of the EM algorithm and its application to parameter estimation for Gaussian mixture and hidden Markov models," *International Computer Science Institute*, vol. 4, p. 126, 1998.

[19] D. Meyer-Delius, C. Plagemann, and W. Burgard, "Probabilistic situation recognition for vehicular traffic scenarios," in *IEEE International Conference on Robotics and Automation 2009. ICRA'09.*, May 2009, pp. 459–464.

[20] J. Firl and Q. Tran, "Probabilistic Maneuver Prediction in Traffic Scenarios (accepted for publication)," in *European Conference on Mobile Robots - ECMR 2011*, 2011.
[21] A. Jaeger, N. Bißmeyer, H. Stuebing, and S. A. Huss, "A Novel Framework for Efficient Mobility Data Verification in Vehicular Ad-hoc Networks (accepted for publication)," *International Journal of Intelligent Transportation Systems Research (IJIR)*, 2011.