Assessment of Node Trustworthiness in VANETs Using Data Plausibility Checks with Particle Filters

Norbert Bißmeyer*, Sebastian Mauthofer†, Kpatcha M. Bayarou*, Frank Kargl‡

*Fraunhofer Institute for Secure Information Technology (SIT), Mobile Networks, Darmstadt, Germany
Email: {norbert.bissmeyer, kpatcha.bayarou}@sit.fraunhofer.de
†Darmstadt University of Technology, Secure Mobile Networking (SEEMOO), Darmstadt, Germany
Email: mauthofer@stud.tu-darmstadt.de
‡Ulm University, Institute of Distributed Systems, Ulm, Germany
Email: frank.kargl@uni-ulm.de

***Abstract*—In Vehicular Ad-Hoc Networks (VANETs), the exchange of location data (i.e. absolute position, heading, time) for traffic safety applications plays an important role. The trustworthiness of this information is crucial as false data affects applications heavily and might endanger human lives. Beside cryptographic solutions that ensure sender authenticity and message integrity, the data plausibility check is an important mechanism to ensure positional reliability. In this paper, we show that a particle filter is an appropriate instrument to perform plausibility checks in order to assess the trustworthiness of neighbor nodes. Our approach allows the aggregation of information from different data sources directly in one particle filter per neighbor. Thus, dependencies and relationships between individual sources can be fully accounted for and the framework is easily extensible and scales well. The concept is implemented as a Java-OSGi bundle for a field operational test framework and evaluated using both manually generated traces and recorded data from real vehicle trips. We show that the detection of several types of location-based attacks is possible under consideration of errors and system inherent deviations in sensor data.**

I. Introduction

VANET communication aims to increase road safety and traffic efficiency by enabling direct message transmission between the network nodes (e.g. vehicles and roadside stations) without having contact to a central infrastructure. This approach is also known as V2X communication and enables on the one hand applications requiring low latency and high message rates but on the other hand allows potential attacks due to the wireless and decentralized network topology. Cryptographic mechanisms allow basic authentication and message integrity verification, but beyond that, the detection of faulty nodes and malicious attackers is still a huge security challenge. Internal attackers that are in possession of valid cryptographic credentials are able to distribute bogus V2X messages in order to exploit the future Intelligent Transportation System (ITS) or simply to disturb its operation.

In V2X, mobility information is broadcasted periodically to all VANET nodes in communication range at a rate of up to 10 Hz using, e.g., Cooperative Awareness Messages (CAMs) [1]. To address the risks caused by nodes sending forged information we propose a misbehavior detection framework based on data plausibility checks. It verifies all incoming mobility information (i.e. absolute GPS position, heading, velocity, timestamp) received with V2X messages. In order to increase the quality of plausibility checking, the framework leverages on different independent information sources that confirm or disprove a specific situation. The position of a neighboring vehicle is for example verified using received mobility data from CAMs sent by the target node and other neighbors, as well as data from vehicle-local sensors (e.g. digital road map, Radar, Lidar, directional antennas). Earlier approaches deployed separate rating modules to process the different information sources as proposed, e.g., in [2], [3], [4], [5]. In this paper we show that the probabilistic particle filter [6], [7] is an appropriate instrument to implement data plausibility checks in VANETs. On the one hand, we are able to combine all available different location information from a broad variety of input sources using only one instance of a particle filter per single-hop neighbor node. On the other hand, our approach benefits from the possibility to directly assesses the trustworthiness of these nodes as shown in Fig. 1.

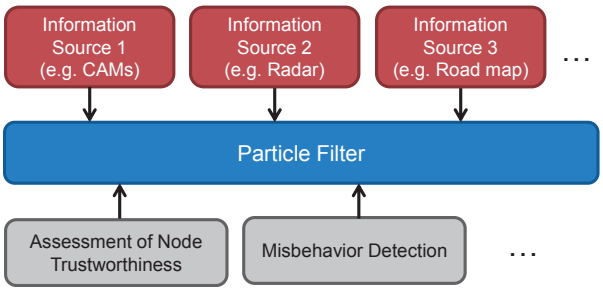


Fig. 1. Data source aggregation and node trustworthiness assessment for data plausibility checking in VANETs using a particle filter

Our strategy allows the weighting of data sources and avoids duplicating information by having only one particle filter per neighbor node. Additionally, we avoid a complex aggregation of information sources and intermediary results that may lead to mutual interference. Nonetheless, the particle filter based plausibility check can be flexibly extended in order to detect inconsistencies introduced by faulty nodes or malicious attackers.

Our approach provides a local consistency check of location-based data in each vehicle. This contrasts with other proposals [8] where vehicles only report information to a central entity that applies then a global consistency checking. There are two main reasons why we advocate the application of data plausibility checks in all vehicles:

1) local applications are directly able to decide whether information from untrustworthy neighbors should be handled with caution without referring to a backend service that might not be reachable at that moment and
2) detected inconsistencies can be filtered much better before being reported to a global misbehavior evaluation authority that would then identify and revoke faulty nodes and attackers.

The paper is organized as follows. In Section II, we present the related work for misbehavior detection and evaluation in VANETs as well as related trust management systems. Section III provides details about the system assumptions and Section IV describes the adversary model. The scheme for misbehavior detection and assessment of node trustworthiness is presented in Section V and VI. In order to show the feasibility of the scheme, Section VII analyzes the functionality and performance under laboratory and real conditions. Finally, Section VIII concludes the paper and gives an outlook for future work.

II. Related Work

As malicious behavior of internal attackers cannot be precluded, the European Telecommunications Standards Institute (ETSI) sees data plausibility checks as an appropriate measure to detect misbehavior based on received message content and sensed mobility behavior [9]. A module based data consistency verification framework is proposed by Schmidt et al. in [3] which uses several location-based modules and gives positive or negative ratings to received message data. A similar approach is discussed in [2] which bases primarily on a probabilistic Kalman filter to track adjacent nodes and detect inconsistencies in their mobility behavior. [2] and [10] show how potential pseudonym changes can be made transparent for a plausibility checker. Kargl et al. propose in [11] the combining of so called Probability Distribution Functions from sensors but without particle filters. Although previous other works are proposing particle filters to increase the node position accuracy in vehicular networks [12], [13], the application of particle filters for data plausibility checking of information sent by neighboring nodes has not been investigated so far. Instead, previous works were typically applying a number of parallel heuristics to verify reported data. [14] is a typical example that proposes various parallel sensors to evaluate position plausibility of VANET nodes for single- and multi-hop communication. Vehicles then calculate a trust value for each neighbor as a weighted average of these sensors. Dötzer et al. also focus on multi-hop communication and likewise determine trust based node evaluations in order to detect attackers in the chain of message forwarders [15].

The principle of node evaluation with *trust* is in general well known and used in different types of network communications. According to Ries [16], trust can be described as the expectation and belief about future behavior, based on experiences and evidences collected in the past, either direct or indirect. Similarly, we describe the trustworthiness of nodes as a pair of two values: *trust* and an associated *confidence*. This concept is originally taken from [17], where the unity of both values is called the *opinion* about a target. A *trust* value corresponds to an estimate of a target's trustworthiness and a *confidence* value, which is also referred to as the quality of the opinion, corresponds to the accuracy of an assigned trust value.

In most of the approaches, detected misbehavior is handled locally in a first instance and may lead, e.g., to the ignoring of untrustworthy data. Beyond the local processing, misbehavior reports can be generated and sent to a central entity in order to identify and exclude or otherwise punish possible attacker nodes. A scheme for central misbehavior report evaluation and attacker identification is presented in [18]. Our approach proposed in this paper is able to provide exactly the information about node trustworthiness that such misbehavior reports require. Both the ETSI [19] and the U.S. Department of Transportation [8] foresee such interfaces for misbehavior reporting in their emerging standards.

III. System Model

The system model of vehicular communications exhibits some characteristics that are VANET specific. Some unique characteristics should be discussed in the following as they have direct influence on the security solutions.

The total number of nodes in the network is determined in general by the number of vehicles and roadside stations that are equipped with wireless transceivers using IEEE 802.11p [20]. After the initial deployment phase several million nodes are to be expected. Following the specifications of ETSI about ITS stations' communications architecture [21], every vehicle will be equipped with at least one Communication and Control Unit (CCU) that acts as router to the wireless network and an Application Unit (AU) that acts as host computer running the applications. All these equipped nodes communicate via direct wireless ad-hoc message transmission in order to archive short latency times and high message distribution frequencies. Every node receives all broadcasted single-hop CAMs from neighboring nodes that are inside its communication range. Additionally, multi-hop messages may be received from distant nodes, whereupon only the mobility information of the last forwarder is used for plausibility checks. In conclusion, a frequently changing network topology must be considered due to high vehicle mobility.

Message authentication and integrity protection is achieved by asymmetric cryptographic signatures and digital certificates that are issued by a commonly trusted Public Key Infrastructure (PKI) [8] [19]. Indeed, this solution successfully prevents network-external attacker, but internal attackers are still a risk that signatures and certificates cannot mitigate. Therefore, a reactive security mechanism for misbehavior detection and attacker identification is necessary that detects inconsistent and incorrect data. For long-term reliability of the network

functionality, faulty or malicious nodes sending such data need to be excluded from the network. In our proposal, every VANET node runs a local data plausibility checker that verifies consistency of incoming mobility data. The main challenges for this reactive security mechanism are: a) the synchronization of used data sources, b) the scalability of the solution due to the possibly large number of neighbors, c) the decentralized character of VANETs and d) the pseudonymity of nodes which may change their temporary identifier frequently.

IV. Adversary Model

We consider an insider attacker that is able to tamper with a vehicle's CCU or AU to make it send V2X messages (e.g. CAMs) that have a valid signature and certificate but where the attacker can still forge the content of the message. An attacker may also be able to extract valid credentials from vehicle CCUs or AUs and then use other devices to send forged messages. By just modifying the mobility data (i.e. absolute position, heading, time) contained in V2X messages, the attacker is able to perform a wide range of location based attacks.

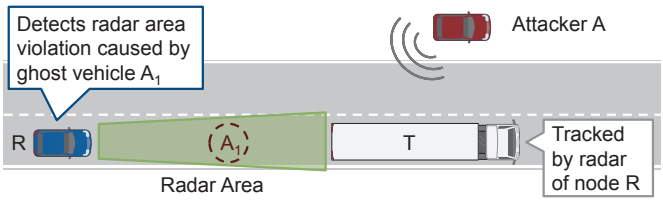


Fig. 2. Attacker model used as basis for mobility data plausibility checks

As shown in Fig. 2, attacker A can misuse the vehicular communication system by sending messages with false mobility data in order to create a non-existent "ghost" vehicle A_1 on the road. We assume that an attacker may even be able to use different identifiers in parallel to create the illusion of several ghost vehicles. As a result, other vehicles (e.g. node R) would assume that a real vehicle A_1 is present at the specified location and time which could trigger false application warnings or other undesired and potentially dangerous system behavior. Besides such roadside attackers with static sending positions, we also assume mobile attackers. However, in both cases, there is a chance that ghost vehicles cause inconsistencies with other information received either in messages from other vehicles or via local sensors. Fig. 2 shows an example where A_1 creates a radar area violation. Vehicle R receives a radar echo from truck T driving in front and is able to determine a radar detection area. Other inconsistencies could be caused by A_1 due to position overlaps with real vehicles on the road, sudden node appearances, map violations or positional jumps. Our approach aims to detect all such inconsistencies based on individual sensors.

V. Position Tracking with Particle Filters

Particle filters belong to the family of Bayesian filters and consist in general of predict / update cycles that are performed repeatedly to estimate the state of a dynamic system from sensor measurements [7]. The first step is the prediction, where a new believe state is calculated based on the prior believe state and a control/input induced transition. The second step is the so called measurement update. Here, the predicted estimate is corrected using sensor observations. The basic idea of particle filters is that any Probability Density Function (PDF) can be approximated by a set of samples. With a sufficient amount of samples, the density of samples in a given area represents the probability of that area. With particle filters, each sample is represented by a particle, containing a whole set of state variables. This enables the sampling of arbitrary density functions and therefore of several complex models.

For the proposed mobility data consistency check a particle filter algorithm using the common Sequential Importance Resampling (SIR) approach is chosen [7]. Each particle $x_t^{[m]}$ is a concrete instantiation of the system state at a time t and represents a sample of the posterior distribution. χ_t is the particle set at time t containing all particles $x_t^{[m]}$ (with $1 \leq m \leq M$) of that time step where M denotes the total number of particles. The belief $bel(x_t)$ reflects the internal knowledge about the state of the environment or the system. In particle filters, the belief is represented by the posterior distribution which is approximated by the set of samples χ_t. For a transition from one belief state to another, it is required that a new control information u_t is available. The transition itself is described by a state transition distribution $p(x_t|u_t, x_{t-1})$. The likelihood for a state hypothesis x_t to be included in the particle set χ_t should be proportional to this distribution.

The algorithm depicted in Fig. 3 takes a set of particles χ_{t-1} together with the most recent control information u_t and the most recent sensor measurement z_t as an input. If no particle set exists yet, a new set with uniformly distributed particles needs to be created first in the initialization phase. Then, two new empty particle sets $\overline{\chi_t}$ and χ_t are created. For normalization purposes, a running counter η is used which sums up all particle weights in the process. The first two steps of the algorithm are performed for each particle in the given particle set χ_{t-1} as shown in Fig. 3: In the sampling step, a new particle $x_t^{[m]}$ is created, based on the knowledge about the control input u_t and the respective particle $x_{t-1}^{[m]}$ of the particle set χ_{t-1}. In order to calculate the required state shift, the state transition distribution $p(x_t|u_t, x_{t-1})$ is sampled.

In the second step, the new particle is weighted. The goal is to correct estimation errors of the prediction using sensor measurements z_t. The weight of a particle $x_t^{[m]}$ is calculated using the conditional probability $w_t^{[m]} = p(z_t|x_t^{[m]})$. This is the probability of the measurement under the condition that the state is according to the given particle. After the weighting is done, the particle is added to a new temporary particle set $\overline{\chi_t}$.

The most important step of the particle filter algorithm is the *resampling* as shown in Fig. 3. The resampling algorithm draws with replacement M particles from the temporary particle set $\overline{\chi_t}$. The probability of drawing a particle corresponds

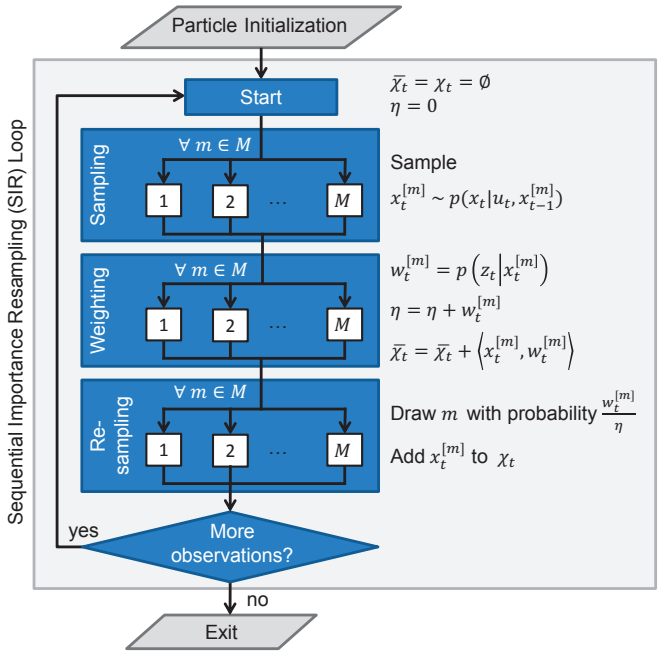


Fig. 3. The particle filter algorithm using sequential importance resampling

to its normalized particle weight $w_t^{[m]}/\eta$. Finally, the drawn particles are added to the output particle set χ_t. Regarding the necessity of the resampling, the following explanation is given in [7]: "The resampling step is a probabilistic implementation of the Darwinian idea of *survival of the fittest*: It refocuses the particle set to regions in state space with high posterior probability. By doing so, it focuses the computational resources of the filter algorithm to regions in the state space where they matter the most." The resulting particle set is used again when a new observation occurs. For further processing each intermediary result could be used as an output of the particle filter.

VI. Trust Based Node Assessment using Particle Filters

In this paper we use a particle filter algorithm to perform a data fusion of several location-related data sources in order to check mobility data plausibility of single-hop neighbor nodes. In our approach, a separate particle filter is used for each tracked vehicle. Particle filters show a high efficiency with respect to tracking purposes and allow the inclusion of negative and positive weighting factors. However, the VANET scenario differs from typical usage scenarios of particle filters where a hypothesis is corrected by fully trusted sensor data values. On the one hand, the incoming position values of the tracked vehicles, which represent an essential part of the "sensor data" used to correct the sampling, can be forged or flawed. On the other hand, the goal of the tracking is not to identify the most likely position itself but to determine the plausibility of the claimed position.

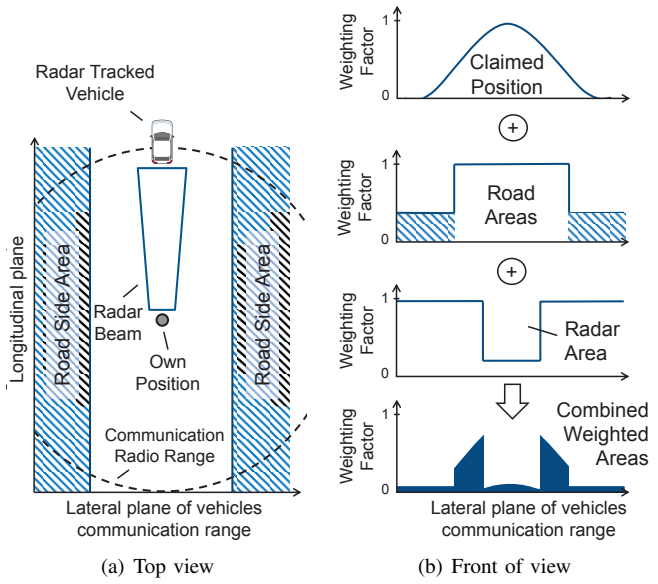
With our proposed particle filter based scheme for plausibility checking of mobility data, we are able to integrate all location verification methods proposed in earlier work:

- Tracking of adjacent nodes to detect position jumps
- Integration of sensor information to confirm or disprove a claimed neighbor node position (e.g. Radar, Lidar, cameras, directional antennas)
- Integration of knowledge to confirm or disprove a claimed neighbor node position (e.g. digital maps, sudden appearance areas [3], maximum communication ranges [2])
- Support of specific checks using the particle filters (e.g. node overlap detection [22], minimum distance moved observation [23], pseudonym change detection [10], tracking of the own position)

A. Data Fusion and Plausibility Checking with Particle Filters

The sampling step of a particle filter is used to predict the state transition from the last state to the current state according to the given control information. In our scheme, the state transition function is based on the positional shift between two incoming messages. From the previous message, the vehicle speed and the direction is derived. This vector is multiplied with the time difference between the previous message and the current message. As the positional shift is assumed to be independent from the absolute current location of the tracked vehicle, all particles are shifted identically. The actual fusion of the different location-related data sources is performed in the weighting step. This step is dedicated to the correction of the prediction from the sampling step. In order to do so, a particle filter is usually fed with sensor data giving hints about the current state of the environment. In our scheme, two types of information are given to the particle filter in order to weight the particles.

The first type of information is the claimed position of the tracked vehicle: This information is taken from the currently analyzed message.



(a) Top view (b) Front of view

Fig. 4. Example to abstract the fusion of multiple weight factors with a primary Gaussian weight distribution

Although this information is not reliable, as it might be forged or faulty, it represents the claimed state of the tracked vehicle. This position is actually the key information which has to be matched with the predicted current position to identify deviations of the movement pattern. If the claimed position does not match at all, there is a high likelihood that the current message is flawed. In order to weight the particles, the information about the claimed position needs to be mapped onto a Probability Density Function. With an increasing distance from the original position, the uncertainty of the claimed position is rising but still a roughly circular shape is generated. The center of the area corresponds to the highest probability and the reduction of probability is approximated by a Gaussian distribution in our current implementations.

The second type of information is locally available data which is assumed to provide reliable additional knowledge about the environment. This involves data obtained by hardware sensors like radar, environmental databases like street maps and general laws of physics, like communication distances. This knowledge is used to decrease the weight of implausible locations and increase the weight of locations with a high likelihood. In Fig. 4(a) and Fig. 4(b), exemplary the influence of road side areas and a radar area is shown in form of colored polygons. These two figures depict the same situation from different perspectives. The top view in Fig. 4(a) shows the own vehicle in the center. The horizontal view from the own vehicle towards the radar tracked vehicle driving ahead is shown in Fig. 4(b). The road side areas alongside the own vehicle's position are decreasing the weight, as vehicles are not assumed to drive off streets. Similarly, the radar area between the own vehicle and the neighbor vehicle running ahead is decreasing the weight for particles located there, as the radar shows this area as free of obstacles. Consequently, particles of a ghost vehicle, claiming its position inside the radar beam area between the own vehicle and the radar detected vehicle in front of, are assigned a low weight.

In principle, every information can be used as a weighting factor as long as it can be described as a single polygon or a combination of multiple polygons that represent the sensor information. In related plausibility check approaches, e.g. [2], [3], each sensor information is used in a separate plausibility check module with possibly redundant code and calculations that each provides one separate confidence value. Our scheme, in contrast, makes it possible to add new knowledge and sensor results in a very simple way. The factor, assigned to each polygon area, represents the importance of the information.

The weighting of particles is done in two steps. First, the bivariate normal distribution of the claimed position is used to weight the particles, then the area factors of the locally available data are applied to increase or decrease the particle weights. That way the claimed position information is dominant in the weighting process. This is required as the next prediction step relies on the information included in the current message. Nevertheless, the area factors can have a high influence on the plausibility rating.

The actual core of the concept is to use the normalization factor of the particle filter as a measurement of the plausibility of the claimed position and therefore of the incoming message. The normalization factor contains the summarized weights of all particles. It is assumed that a high particle weight - which results either from closeness to the center of the bivariate normal distribution or from a positive area factor - represents a high likelihood of being in a plausible state. Accordingly, a low particle weight results from high uncertainty and this is likely caused by conflicting information. Therefore, a high normalization factor (= high probability) is caused by a large number of high rated particles, and a low factor (= low probability) by many low rated particles - with a smooth transition between the two extremes.

B. Assessment of Node Trustworthiness

This normalization factor is now used to assess the trustworthiness of neighboring nodes. As mentioned in the related work in Section II, we are using a pair of two values (i.e. trust and confidence) in order to assess the trustworthiness of neighbor nodes. Furthermore, we separate between a *message trust* value T_m and a *vehicle trust* value T_v as detailed in Section VI-B1 and VI-B2 respectively. Trust values $T \in \mathbb{R}$ and associated confidence values $C \in \mathbb{R}$ are assigned to the range $[0; 1]$. A value of 1 represents the best possible rating, a 0.5 indicates missing knowledge or uncertainty and 0 is the worst possible rating. The transition is fluent. In order to calculate the message trust value, we map the normalization factor Ω of the particle filter onto a scale of $0 \leq x \leq 1$ with $x \in \mathbb{R}$. In order to do so, the upper limit of Ω needs to be evaluated using training data primarily. Due to the stochastic character of the particle filter and sensor noise, a number Ω' with $\Omega' < \Omega$ is selected to match the maximum in the mapping. Numbers greater than Ω' are mapped to the maximum value 1 as well. In the simplest way a linear mapping function could be used, where $\Omega'/2$ will be mapped to value of 0.5.

If, e.g., the maximum measured total particle weight is 100, we map the 1 to a value of about $\Omega' = 80$ and therefore the 0.5 to a value of $\Omega'/2 = 40$. In the same way, measured values like 20 and 60 would result in ratings of 0.25 and 0.75 respectively. A more sophisticated mapping function that may be applied in a live system, could be investigated in future work.

1) Message Trust: The message trust value T_m is an indication of the trustworthiness of the currently analyzed message. A high value is usually achieved if the bivariate normal distribution of the claimed position is centered above a large portion of the particles while the influence of negatively weighted areas is only minimal. Therefore, the vehicle movement is in accordance with the prediction and own sensor measurements as well as rules do not indicate a violation. Any deviation from this state will result in a gradual decrease of the trust value. Low trust values can be the result of unforeseen movement patterns and/or violations of other plausibility checks, represented by the weighted areas. Although a low value might indicate a potential attack, it is

also possible that it is caused by jumpy GPS signals, sudden driving maneuvers and other natural reasons.

2) Vehicle Trust: The vehicle trust value T_v contains the history of previous message trust values. It is an indication of the general vehicle trustworthiness, i.e. the real existence of the vehicle on the road. The value is calculated by exponentially averaging previous message trust values:

$$T_v = T_v * (a - 1) + T_m * a \quad (1)$$

The aging factor $a \in [0; 1]$ determines the ratio of how much a new message trust value affects the vehicle trust. The starting value of T_v is 0.5 which indicates that no prior knowledge about a tracked vehicle is available. If a sufficiently low value (< 0.1) for a is chosen, it takes several messages to reach a very high or very low vehicle trust. A single bad message trust rating will only effect the vehicle trust marginally, but multiple successive bad ratings will lead to a rapid decline of the vehicle trust.

3) Vehicle Trust Confidence: The purpose of the vehicle trust confidence C_v is to confirm the vehicle trust T_v. If the confidence value is low, either too little information has been collected about a target node or a rapid change of T_v is happening. In both cases it would be wise not to trust in T_v. Therefore, the vehicle trust confidence value represents the confidence of the system that the vehicle trust value is correct. Alternatively, it can be described as the quality of the vehicle trust value. Equation 2 is used for the calculation of C_v, with $\overline{T_m}$ being the average value of the last X message trust values.

$$C_v = 1 - |T_v - \overline{T_m}| \quad (2)$$

Besides being used as a confirmation of the plausibility of T_v, the vehicle trust confidence can also be used to suspect potential attacks, as low values of C_v indicate a sudden change of the vehicular behavior. For example, a low value can be caused by a faked vehicle suddenly entering an area which is free from vehicles, according to the radar sensor.

C. Misbehavior Detection with Particle Filters

Besides the usage of the particle filter to assess the trust values based on the normalization factor, there are other possibilities to make use of the particle filter.

On the one hand, it is possible to check if an object at a given location is matching with the particle cloud of one of the tracked vehicles. This mechanism can be used to test if any of the tracked vehicles is the one detected by the radar or if a tracked vehicle has performed a pseudonym change and appears subsequently with a new identifier. On the other hand, the particle cloud could be used to check whether the claimed position of neighboring vehicles overlap. As two or more vehicles should not be at the same location at the same time, this could be used to identify suspicious vehicles.

Finally, an additional particle filter could be used to track the own vehicle position. It does not matter if imprecise map data, winding roads, or an inaccurate own position is the cause, the own vehicle should always be able to serve as a reference with respect to plausibility. If the own vehicle is not able to achieve a good vehicle trust value, the whole plausibility check should be suspended.

VII. Evaluation

In order to evaluate the usability of particle filters for plausibility checking and node trustworthiness assessment in VANETs, we performed several tests with hardware and software from the field operational test sim^{TD} [24]. Initially, the quality of our particle filter based plausibility check is measured, followed by performance evaluations. A Java OSGi implementation of the data plausibility check has been integrated into the AU of the sim^{TD} system. The OSGi framework runs on a car PC with an Intel Atom D510 processor at 1.66 GHz and 2 GB of RAM.

A. Quality of Node Trustworthiness Assessment

In Section VII-A1, we use different manually generated vehicle traces that are replayed under laboratory conditions. After that, we show the practicability of our scheme under real condition, where three vehicles from the sim^{TD} project were used to drive various maneuvers on a testing area as described in section VII-A2. For the following evaluations we used one particle filter per neighboring vehicle. Each filter contains 1000 particles, has a filter area size of 800×800 meters and uses the aging factor $a = 0.06$, as applied in Eqn. 1. In order to indicate suspicious behavior thresholds are used.

1) Tests under Laboratory Conditions: The test results shown in Fig. 5 present the attack discussed in Section IV: A tracked ghost vehicle A_1 drives along with the vehicle R that runs the plausibility checker. At the beginning A_1 moves

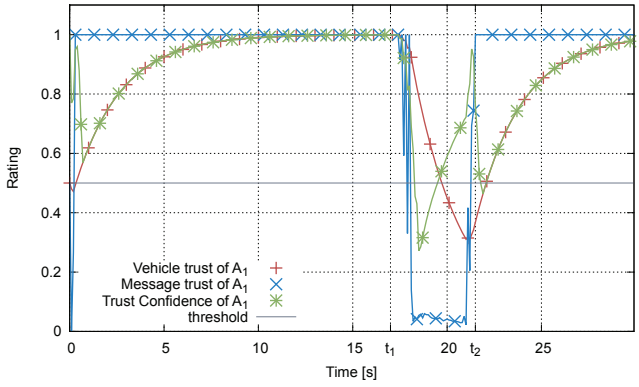


Fig. 5. Trust and confidence values of a simulated trace with radar area violation

with a constant speed, identical to the speed of R, and keeps a constant distance. After a while, the tracked ghost vehicle enters the radar area that is spanned between the vehicle R and another real vehicle T that is detected by the radar. As it is very unlikely that a real vehicle exists in the radar-monitored area, this area is given a weighting factor of 50, which will result in a particle weight reduction of $\frac{1}{50}$.

As shown in Fig. 5 the vehicle trust value will increase rapidly after the initialization phase and stay at a high level until the vehicle enters the radar area at time t_1. As expected,

the message trust suddenly drops to a low value and the vehicle trust confidence drops to a value below 0.5 shortly and then increases again as the vehicle trust decreases. It has to be considered that the confidence C_v has high values if the difference between message trust values and vehicle trust values is small. While the ghost vehicle is within the radar area, the vehicle trust value declines. Shortly after the ghost vehicle leaves the radar area at time t_2, the message trust reaches a high value again and the vehicle trust increases as well. As the vehicle trust confidence indicates uncertainties in the trust measurements, the confidence value shortly drops below the threshold of 0.5 and then rises again to its maximum. Fig. 5 shows that the malicious behavior of the ghost vehicle A_1 is clearly detected due to the decrease of vehicle trust and message trust values caused by violation of the radar area.

2) Tests under Real Conditions: The tests under real conditions are based on real traces recorded on a dedicated test area where several simple maneuvers, like sudden braking and evasion of obstacles were performed. The test results shown in Fig. 6 address the impact of radar object detection similar to the tests under laboratory conditions. The tracked ghost

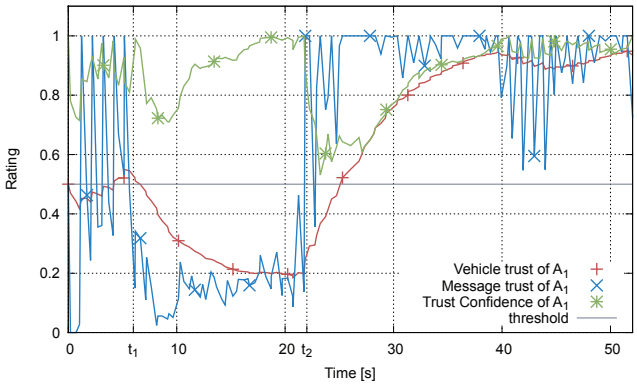


Fig. 6. Trust and confidence values of a real overtaking maneuver with radar area violation

vehicle A_1 starts a sudden overtaking maneuver and cuts in the gap between the vehicle R and a heading vehicle T at time t_1. Afterwards, at time t_2 the ghost vehicle leaves the radar area but stays in communication range and performs some further driving maneuvers. Fig. 6 shows the decrease of vehicle trust and message trust below the threshold at time t_1 which indicates non plausibility behavior of the tracked vehicle A_1. Similar to the test results under laboratory conditions, the vehicle trust increases as soon as the ghost vehicle leaves the radar area at time t_2. In spite of jumpy message trust values caused by abrupt driving, the expectations are fulfilled.

Therefore, we can show that the particle filter algorithm is able to handle real vehicle data without giving wrong warnings under typical driving behavior. At the same time, attacks according to our attacker model can be detected reliably.

B. Accuracy and Performance of the Particle Filter

As the quality of the plausibility check is directly related to the number of particles in the filters, we analyzed the accuracy and performance using our vehicle traces. The optimal number of particles is always dependent on the use case and its requirements. An increase of particles leads to a higher accuracy but needs more processing power. Fig. 7 presents vehicle trust graphs for multiple different numbers of particles, starting from 10 particles up to 1000 particles. For these performance evaluations, we reused the recorded real vehicle traces presented in Section VII-A2. As reference for the accuracy evaluation we use the graph for vehicle trust of A_1 shown in Fig. 6. All graphs depicted in Fig. 7 that exhibit small deviations from the reference vehicle trust graph can be assumed to have appropriate particle numbers.

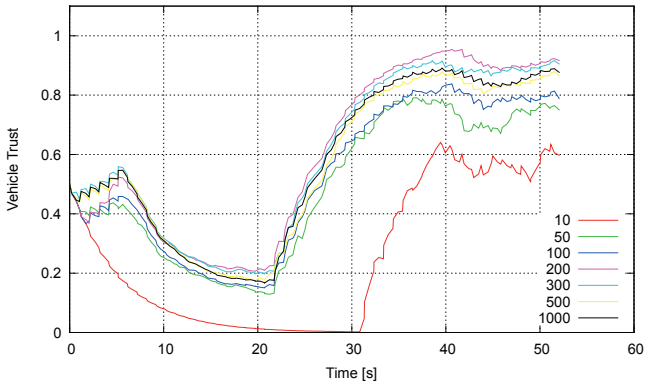


Fig. 7. Accuracy of measurements with different numbers of particles

The best results can be achieved with particle numbers between 500 and 1000. The graphs of those two particle numbers are nearly identical and centered within the other graphs. In theory, a particle filter using more particles should produce better results as it should converge to the optimal solution. However, in our tests we have observed that filters with more than 2000 particles cannot be processed fast enough due to limited processing power on our automotive system. With less than 300 particles, the results are still usable but get less and less accurate. For reliable results, 100 particles should be the lower bound.

Fig. 8 shows the performance measurements of the particle filter with varying numbers of particles similar to the accuracy evaluation shown in Fig. 7. As the complexity of particle filters is $O(M)$, an increase of particles causes a linear increase of computational effort, which might be a problem in resource restricted environments. Using only 100 particles per particle filter, it would be possible to handle up to 200 incoming messages per second. Using between 500 and 1000 particles per filter, approximately 40 messages can be processed. Consequently, the particle filter algorithm may be adapted to incoming message rates and only relevant neighbors may be tracked.

VIII. Conclusion and Outlook

As motivated in Section 1, the detection of insider attackers is an important requirement for trustworthy V2X communication and therefore we propose a data plausibility verification

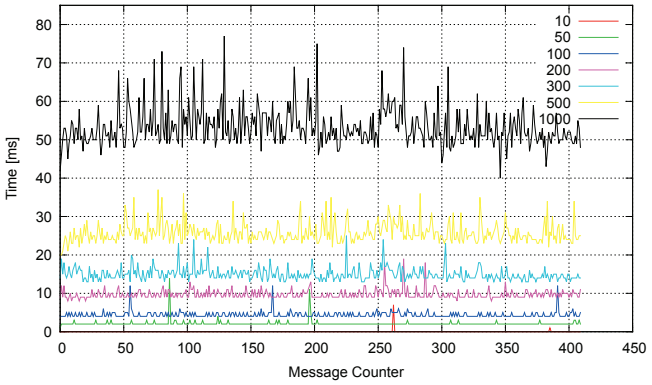


Fig. 8. Runtimes of the particle filer algorithm in dependence of the number of particles

scheme that is based on particle filters. Our framework is able to process different types of information sources in order to assess the trustworthiness of neighbor nodes. The result of the particle filter can be used locally to adapt directly the processing of messages from untrustworthy neighbors. On the other hand, the data of the particle filter can also be used to generate misbehavior reports that are processed by a central entity in order to globally identify and exclude attackers. The handling of particle filters is easy and can be extended with additional different data sources in order to increase the quality of misbehavior detection. As shown in our tests under laboratory conditions, the approach allows to detect inconsistencies reliably while providing a low false positive rate. Additionally, tests under real conditions show that the plausibility check can cope with data inaccuracies and real driving maneuvers. Finally, the performance measurements demonstrate that at least 200 messages per second can be processed using field operational test hardware and software.

In future work, a context sensitive runtime update of the particle filter might be an option to further increase its quality and performance.

ACKNOWLEDGMENT

This work was supported by CASED (www.cased.de) and has received funding from the European Union's Seventh Framework Programme project PRESERVE under grant agreement n°269994.

REFERENCES

[1] ETSI - European Telecommunications Standards Institute, "Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," ETSI, Technical Standard TS 102 637-2, April 2010.

[2] H. Stübing, A. Jaeger, N. Bißmeyer, C. Schmidt, and S. A. Huss, "Verifying mobility data under privacy considerations in Car-To-X communication," in *ITS World Congress*, vol. 17th ITS World Congress, Busan, October 2010.

[3] 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.

[4] T. Leinmüller, E. Schoch, and F. Kargl, "Position verificiation approaches for vehicular ad hoc networks," *Wireless Communications, IEEE*, vol. 13, no. 5, pp. 16 –21, October 2006.

[5] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications*, vol. 31, no. 12, pp. 2883 – 2897, 2008, mobility Protocols for ITS/VANET.

[6] K. Hsiao, J. Miller, and H. de Plinval-Salgues, "Particle filters and their applications," *Cognitive Robotics, April*, 2005.

[7] S. Thrun, W. Burgard, and D. Fox, *Probabilistic Robotics*. Cambridge: MIT Press, 2005.

[8] U. D. of Transportation Research and I. T. Administration, "Security credential management system design security system design for cooperative vehicle-to-vehicle crash avoidance applications using 5.9 ghz dedicated short range communications (dsrc) wireless communications," CAMP, VSC3, www.its.dot.gov, Tech. Rep., February 2012.

[9] ETSI - European Telecommunications Standards Institute, "Intelligent transport systems (ITS); security; threat, vulnerability and risk analysis (TVRA)," ETSI, Technical Report TR 102 893, March 2010.

[10] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on*, feb. 2010, pp. 176 –183.

[11] F. Kargl and A. Bernauer, "The compass location system," in *First International Workshop on Location- And Context Awareness (LoCA 2005)*, vol. 3479/2005. Oberpfaffenhofen, Germany: Springer LNCS 3479/2005, May 2005, pp. 105–112.

[12] M. Efatmaneshnik, A. Balaei, N. Alam, and A. Dempster, "A modified multidimensional scaling with embedded particle filter algorithm for cooperative positioning of vehicular networks," in *Vehicular Electronics and Safety, 2009 IEEE International Conference on*. IEEE, 2009.

[13] Z. Khan, T. Balch, and F. Dellaert, "An mcmc-based particle filter for tracking multiple interacting targets," *Computer Vision-ECCV 2004*, pp. 279–290, 2004.

[14] T. Leinmüller, C. Maihöfer, E. Schoch, and F. Kargl, "Improved security in geographic ad hoc routing through autonomous position verification," in *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*. ACM, 2006, pp. 57–66.

[15] F. Dötzer, L. Fischer, and P. Magiera, "Vars: A vehicle ad-hoc network reputation system," in *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*. IEEE, 2005, pp. 454–456.

[16] Ries, "Certain trust: A trust model for users and agents," in *SAC '07: Proceedings of the 2007 ACM symposium on Applied computing*. New York, NY, USA: ACM, 2007, pp. 1599–1604.

[17] G. Theodorakopoulos and J. Baras, "Trust evaluation in ad-hoc networks," in *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 1–10.

[18] N. Bißmeyer, J. Njeukam, J. Petit, and K. Bayarou, "Central misbehavior evaluation for vanets based on mobility data plausibility," in *VANET '12: International workshop on Vehicular inter-networking*. ACM, April 2012.

[19] ETSI - European Telecommunications Standards Institute, "Intelligent transport systems (ITS); security; security services and architecture," ETSI, Technical Standard TS 102 731, September 2010.

[20] IEEE Computer Society, "IEEE standard for information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – Part II: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," IEEE Std 802.11p, Tech. Rep., 2010.

[21] ETSI - European Telecommunications Standards Institute, "Intelligent transport systems (ITS); communications architecture," ETSI, European Norm EN 302 665, September 2010.

[22] N. Bißmeyer, C. Stresing, and K. Bayarou, "Intrusion detection in VANETs through verification of vehicle movement data," in *Second IEEE Vehicular Networking Conference*. IEEE, December 2010.

[23] R. Schmidt, T. Leinmüller, and A. Held, "Defending against roadside attackers," in *16th World Congress on Intelligent Transport Systems*, Stockholm, Sweden, September 2009.

[24] C. Weiß. (2011, October) Safe and intelligent mobility test field germany. Project Presentation. Daimler AG. http://www.simtd.de.