Decentralized Position Verification in Geographic Ad Hoc Routing

Tim Leinmüller[+], Elmar Schoch[*], Frank Kargl[*] and Christian Maihöfer[**]
[+]DENSO AUTOMOTIVE Deutschland GmbH, Technical Research Department, t.leinmueller@denso-auto.de
[*]Ulm University, Institute of Media Informatics, {elmar.schoch|frank.kargl}@uni-ulm.de
[**]Daimler AG, Group Research and Advanced Engineering, christian.maihoefer@daimler.com

Abstract

Inter-vehicle communication is regarded as one of the major applications of mobile ad hoc networks (MANETs). Compared to MANETs or wireless sensor networks (WSNs), these so called vehicular ad hoc networks (VANETs) have unique requirements on network protocols. The requirements result mainly from node mobility and the demands of position-dependent applications. On the routing layer, those requirements are well met by geographic routing protocols. Functional research on geographic routing has already reached a considerable level, whereas security aspects have only been recently taken into account. Position information dissemination has been identified as being crucial for geographic routing since forged position information has severe impact regarding both performance and security.

In this work, we first summarize the problems that arise from falsified position data. We then propose a framework that contains different detection mechanisms in order to mitigate or lessen these problems. Our developed mechanisms are capable of recognizing nodes cheating about their position in beacons (periodic position dissemination in most single-path geographic routing protocols, e.g. GPSR). Unlike other proposals described in the literature, our detection system does not rely on additional hardware or special nodes, which would contradict the ad hoc approach. Instead, we use a number of different independent sensors to quickly give an estimation of the trustworthiness of other nodes' position claims. The different sensors run either autonomously on every single node, or they require cooperation between neighboring nodes.

The simulation evaluation proves that the combination of autonomous and cooperative position verification mechanisms successfully discloses most nodes disseminating false position information, and thereby widely prevents attacks using position cheating.

I. Introduction

In the recent years, Mobile Ad hoc Networks (MANETs) have attracted a lot of attention in the research community. Still, there are very few real application scenarios where the wide deployment of MANETs is really foreseeable in the near future. Two exceptions are the military area and networks that spontaneously connect vehicles on the road, so called Vehicular Ad hoc Networks (VANETs). In the latter case, a number of research projects produced significant results concerning routing and other operational issues (e.g. projects like Fleetnet [1] or CarTalk2000 [2]). Main target of these projects is the improvement of vehicle safety by means of inter-vehicle communication. In the case of an accident, a VANET might for example be used to warn approaching cars and give the drivers enough time to come to a halt. Another application area is using VANETs for entertainment purposes, allowing e.g. news exchange between passengers of different cars.

Now European and US vehicle manufacturers are taking the next step in projects and standardization bodies that aim at defining a reference architecture and suitable standards for VANETs, e.g. in the US Vehicle Safety Communication Consortium (VSCC) [3], the Car2Car Communication Consortium (C2C-CC) [4], or the Network on Wheels project (NoW) [5].

In contrast to generic MANETs, where mostly topology-based routing protocols are being developed, many of the VANET projects use so called position-based routing. This approach, which is also called geographic routing, offers significant advantages for VANETs and has therefore attracted a lot of research.

Many VANET applications need to distribute their data based on the geographic position of destination nodes. This form of addressing, called Geocast, can easily be implemented when using geographic routing

protocols. Furthermore, car-to-car networks show high node mobility and contain potentially large numbers of nodes. Geographic routing is able to address these challenges better than topology-based protocols [6]. One reason is that topology-based protocols like DSR [7] or AODV [8] need to find and maintain routes, which is not necessary for geographic routing. The matter of position determination is not a critical issue in vehicular ad hoc networks, due to the increasing number of cars being equipped with GPS receivers, which is mostly used in navigation systems.

An overview on position-based routing schemes for mobile ad hoc networks using the individual node position can be found in [6]. For VANETs, most commonly *greedy routing* approaches have been selected. They have in common that the next hop node of a packet has to be closer to the destination's position than the current node. This implies that a node has to know all its neighbors and their respective position, which is achieved by all nodes sending a periodic broadcast of their own position. By this so called *beaconing* every node can build up a neighbor table and base forwarding decisions on it. Two special cases must be handled with greedy forwarding: there may be more than one suitable next hop or there may be no suitable neighbor.

*C*ached *G*reedy *Geoc*ast (CGGC) specifically addresses these two cases respecting the special needs of VANETs [9]. In CGGC, the first case as mentioned above is addressed using the neighbor with the minimum Euclidean distance to the target. If no suitable next hop is found, the packet is cached to be forwarded at a later time. This strategy is based on the assumption of high node mobility in VANETs which makes it likely to encounter a suitable next hop soon.

While position-based routing protocols like CGGC are very robust under high mobility, there is one critical issue. When nodes send false position information in their beacon messages, this can severely impact the performance of the network [10], [11]. A potential source for such false position data is a malfunction of a node's location sensing system. E.g. a GPS receiver may wrongly calculate the position of a node because of bad reception conditions.

Whereas malfunctioning nodes may degrade the performance of a system to some extent, malicious nodes may cause even more harm. The intents of an adversary may range from simply disturbing the proper operation of the system to intercepting traffic exchanged by ordinary users, followed by a potential modification and retransmission. If the data is not protected against modification or eavesdropping, e.g. by cryptographic means, this can lead to a compromise of security goals like confidentiality, authenticity, integrity, or accountability.

In [10] and [11] we have analyzed the effects of position faking nodes in different scenarios (city and highway). In [12] we have proposed a set of autonomous and cooperative mechanisms that enable position verification. The autonomous mechanisms have been studied in detail in [13]. In this work, we provide a complete view on the problem and our proposed solution and we complement previous work with more details on cooperative sensors.

The remainder of this paper is organized as follows. After briefly summarizing the effects of false position data in the next section, we describe related work regarding countermeasures in section III. Then, section IV introduces our verification mechanisms, divided into autonomous sensors and cooperative sensors, as well as a framework for the combination of results of different sensors. Section V presents the results of the simulative analysis we have conducted in order to confirm the mechanisms' applicability, especially under consideration of the requirements in VANETs. Furthermore, the analysis of the verification contains a second part that elaborates on weaknesses of and potential attacks against our verification system. Finally, we summarize the main achievements of our work and conclude with section VI.

II. Effects of Falsified Position Information

This section summarizes the influence of false position data generated by malfunctioning or malicious nodes on geographic routing. In [10], we have discussed all potential situations that can occur when a node transmits false position information in beacon messages. Then we focused on the influence on routing in city scenarios. For highway scenarios we did a similar analysis in [11].

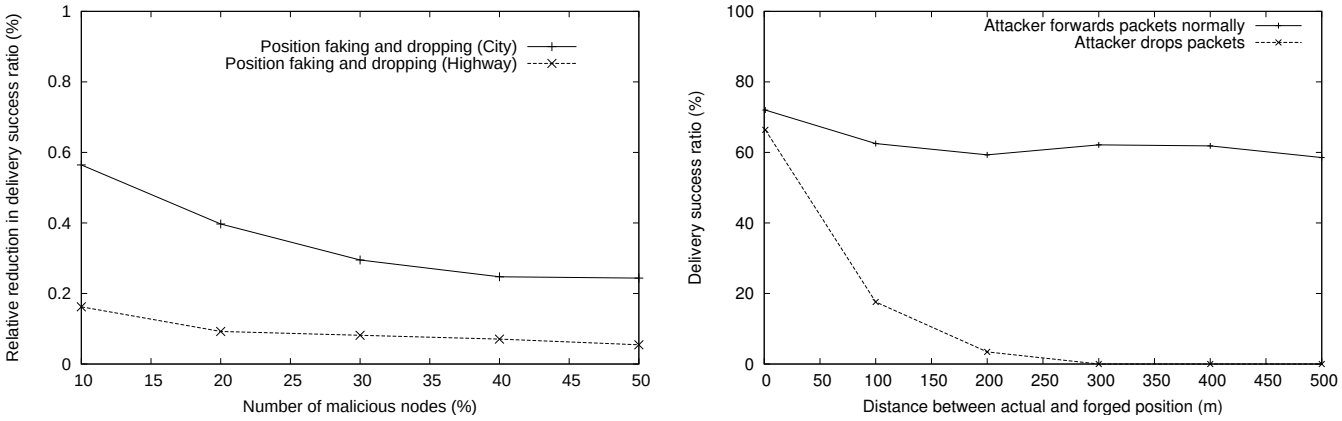

Fig. 1. a) Relative reduction in successfully delivered messages depending on number of malicious nodes(city compared to highway scenario), b) delivery success ratio if a single attacker dedicatedly falsifies its position (highway scenario)

Both analyses show, false position data is clearly an issue that can affect the performance, reliability and security of any network that uses position-based routing. The impact of falsified position data on routing has been evaluated using the ns-2 simulation environment, with the same routing algorithm and attacker model that is described in detail later in section V-A.

The simulation results show that in highway scenarios the impact is more severe than in city scenarios (see figure 1a). In general highway scenarios, position faking can result in an overall delivery ratio decrease up to approximately 90%, relatively independent of the number of maliciously acting nodes in case theses nodes drop intercepted packets. In the special case where all packets have to traverse an area with a single stationary attacker, delivery ratio even decreases to zero, as shown in figure 1b. In city scenarios the overall delivery ratio might decrease up to approximately 70%, depending on the number of maliciously acting nodes and depending on whether the malicious nodes drop packets or not.

The reasons for decreased delivery ratio depend on the forwarding behavior of malicious nodes. Whereas for scenarios without packet dropping by position faking nodes, decreased delivery ratio results from routing loops, in scenarios with packet dropping by position faking nodes, the dropping itself is of course the actual reason.

III. Related Work

Whereas a lot of effort was already put in securing traditional MANETs [14], [15], the security research for position-based routing and VANETs is still in its infancy. [16] gives a first overview on this subject. When using position-based routing, one important aspect is the correctness of position data. The routing mechanisms proposed so far all work the same: nodes measure their location by means of some sensors (e.g. GPS) and then distribute the measured location to other nodes which can then base their routing decision on the location of others.

Greedy routing and some applications for VANETs depend on reliable neighbor positions. Yet, the term ”reliability” implies that a node cannot influence the position information given in beacons of neighboring nodes. Assuming all nodes working properly and no nodes trying to act maliciously, there is no reason for intervention. But effectively, neighbors may claim a falsified position and thereby can carry out several attacks, like node isolation or packet interception [10].

The only solution to a position falsification attack method is to introduce some kind of position verification. Some approaches to verify node positions take up the basics of positioning systems. They use angle or distance measurement techniques like radio signal strength or time of flight, partly in combination with challenge-response procedures to approve position claims secure and unambiguously.

For instance, the verification system described in [16], [17] contains base stations building a trustworthy network. In the approach called *Verifiable Multilateration*, four of these base stations are involved in every

position verification procedure. One after another, each of these stations measures the time between sending a challenge to the corresponding node and the arrival of the answer. Therefore a node might enlarge its actual distance to a base station by delaying the answer, but it has no possibility to reduce it (i.e. the node cannot send the answer to the challenge in advance), because the node does not know the challenge before actually having received it. In case a node delays the answer and thus enlarges the distance to one of the base stations, this is discovered by a misleading multilateration when looking at all four distance measurements.

The approach can be improved by using synchronized base stations. Then only one challenge message is necessary; the distance can be measured at every involved base station simultaneously. The gain in verification speed is payed with the disadvantage that a node with sectoral antenna can send out the answers to each base station with temporal delay and so is able to trick the verification.

Other approaches confine themselves to verify that a node resides within a defined region, e.g. for location based access control. The solution in [18] places so called *verifiers* at special locations and defines an acceptable distance for each verifier. Thus a region R can be formed by overlapping circles. The verification procedure then works as follows. First, the corresponding node n sends out a beacon containing its position. Then a verifier v replies with a challenge via radio. After receiving the challenge, n has to answer via ultrasound. If the answer arrives at v in the previously calculated time according to the defined acceptable distance for v, n is approved to be within the region R.

Whereas [18] only works with special hardware, a similar approach in [19] achieves position verification simply based on logic reception of beacons. First, the verifier nodes are divided in acceptors and rejectors. The acceptor nodes are distributed over the region R which is to be controlled. Then, a closed annulus with rejector nodes is formed around the acceptors. In addition to the distinct placement, verifier nodes are synchronized among each other. Nodes send the same beacon multiple times with increasing transmission power. If a transmission of this beacon is first received by an acceptor, the position claim is accepted, if its first received by an rejector, the position claim is rejected.

Summarizing related work, there are mainly two groups of position verification approaches. The first group of solutions tries to measure physical parameters like Time of Arrival (TOA), Angle of Arrival (AOA), Time Difference of Arrival or the received signal strength [16], [17], [18]. Other approaches do not rely on physical measurements but rather try to verify the position claims of other nodes based on the logical structure of the network [19].

IV. Position Verification Approach

The previously described systems either require specific hardware or rely on an infrastructure of verifiers to validate the positions. For VANET scenarios, these assumptions are not likely to be fulfilled.

Our goal is to design a system that works completely without infrastructure or dedicated hardware. We use the concept of a "Position Cheating Detection System" similar to intrusion detection systems in MANETs, e.g. [20]. In these systems every node uses multiple algorithms (so called sensors) to detect malicious or selfish behavior of other nodes in the network. Based on the sensors' observations, each node calculates a trust value that determines whether other nodes are trustworthy, or should for instance be excluded from further routing decisions. Such systems can predict the trustworthiness of other nodes even when single sensors do not work fully reliable.

We transfer this idea into the domain of position verification. Therefore it is necessary to find suitable sensors that can be used to detect forged position information. There are two classes of position verification sensors. Sensors of the first class work autonomously on each node and contribute their results to the node's local trust rating of neighbors. The second class includes all sensors that work in cooperation with other nodes, thus requiring additional communication between the nodes. Figure 2 gives an overview on sensors from both classes that will be discussed in detail in this paper.

All these sensors have the benefit that they rely only on information that is delivered by the routing layer, there is no additional hardware required. We assume that the nodes in the VANET use a location-

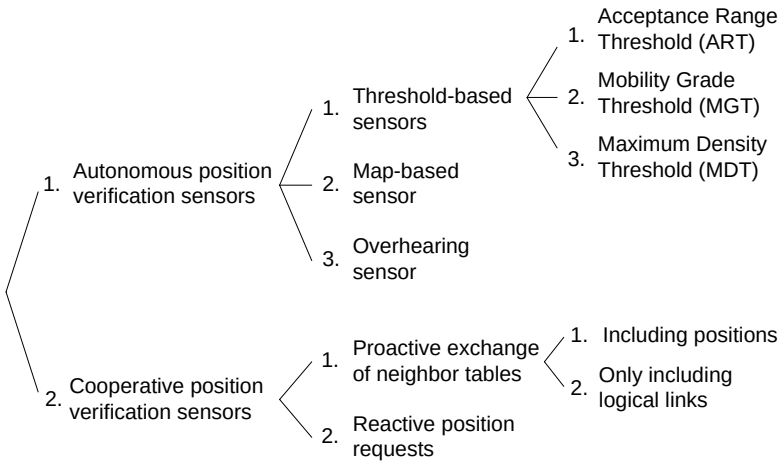

Fig. 2. Position verification sensors overview

based routing protocol like the one described in [9]. This implies that every node is able to determine its current position, e.g. by using a (D)GPS receiver.

In the routing protocol, location information is distributed between nodes by means of position beacons. Beacons need to be signed and timestamped by their sender in order to prevent impersonation and replay. When a node receives a position beacon from another node claiming to be at a certain position, the sensors get active to verify if this claim is likely to be correct or not.

Next we describe the way the verification system combines the results from different sensors over time. Then we introduce sensors from both classes, first the autonomous sensors, then the cooperative sensors. At the end of this section, we compare the different sensors and elaborate on their advantages as well as their disadvantages.

A. Combination of Verification Results

To provide a decision whether a node should be regarded as being malicious or not requires that observations are aggregated over time and from different sensors. Also knowing that observations from some sensors are more reliable than observations from others, we use a trust model that provides the capabilities to consider observations from differently weighted sensors during a certain period of time. The mathematical model is derived from the one presented in [21].

We denote the n-th observation of sensor s by σ_n^s. Then, the trust model can be described as follows:

- All nodes store trust values $r \in [-1; 1]$ for all direct neighbors. $r = 0$ is equivalent to neutral trust, $r \in (0; 1]$ means a node is trustworthy and $r \in [-1; 0)$ means no trust.
- Every observation σ_n^s is stored with weight factor w^s and timestamp t_n^s.
- On the arrival of a new observation, the trust value for a neighboring node is recalculated according to the collected observations for this node.
- All observations are stored for a maximum time T and discarded afterwards.

The weight factor w^s of an observation σ_n^s is chosen according to the reliability of the respective sensor. Observations, for example from a more reliable sensor like ART can be weighted higher than observations from less reliable sensors like MGT. In addition, observations may also be weighted dynamically, for instance depending on traffic situation or the current scenario.

The timestamp t_n^s of an observation σ_n^s is used to calculate the observation's time factor $wt(t, t_n^s)$,

$$wt(t, t_n^s) = 1 - \left(\frac{t - t_n^s}{T}\right)^x \tag{1}$$

where x denotes the exponential aging factor of the observations. $x = 1$ corresponds to a linear aging process, values $x > 1$ are equivalent to a more than linear aging process of the respective observation.

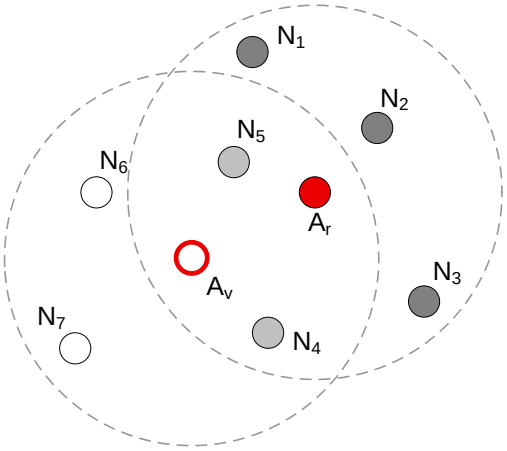

Fig. 3. Acceptance Range Threshold (ART) example

Finally, the trust value r_t of a neighbor node at a time t is calculated by multiplying the available observations by their weight factor and their time factor, then summarizing the results and at the end normalizing to $[-1; 1]$,

$$r_t = \sum_{i \in S} w^i \sum_{j \in N_i} wt(t, t_j^i) \;\; \sigma_j^i \Bigg|_{-1}^{1} \tag{2}$$

where S denotes the number of sensors s, and N_s the number of collected observations by sensor s. This calculations is repeated when a new sensor observation is available.

Detected violations are weighted higher than normal behavior, thus once a falsified position information is detected, it takes several correct beacon messages to compensate the trust level. Nodes with a negative rating are not used for forwarding.

B. Autonomous Sensors

1) Acceptance Range Threshold: The Acceptance Range Threshold (ART) sensor is based on the observation that all radio networks have a maximum communication range where packets sent by a node B still can be received successfully by a node A. Based on the radio used in VANETs, we define a fixed maximum acceptance range threshold ΔMax for the ART sensor.

By disregarding position beacons from nodes claiming to be at a distance larger than ΔMax away from a receiving nodes' current position, we avoid many types of attacks. Using this simple method, for instance, a node A cannot easily collect all outgoing traffic of another node B by pretending to be at a better forwarding position, i.e. closer to remote targets, than potential other nodes in the direct neighborhood.

The consequences are shown in Figure 3. Position beacons from node A, being at the real position A_r but claiming to be at position A_v will be rejected by nodes N_1 through N_3 as the ART is exceeded. On nodes N_6 and N_7 on the other hand, the sensor would not reject the beacons, but due to the limited radio range, N_6 and N_7 do not receive beacons from A anyway. Additionally, the ART mechanism does also prevent routing loops that false position information can create in many greedy routing strategies as shown in [10].

2) Mobility Grade Threshold: The Mobility Grade Threshold (MGT) is based on the assumption that nodes can move only at a well-defined maximum speed. Depending on the scenario, this may be the general speed-limit on streets (plus a bonus for speeding cars) or the maximum walking speed of persons. The sensor works as follows. Nodes record a timestamp in addition to every received beacon. When receiving subsequent beacons from the same node, the receiving node is able to verify whether the average speed

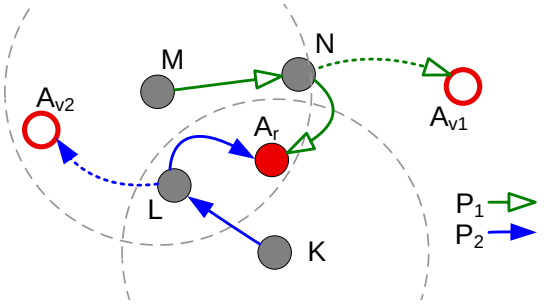

Fig. 4. Mobility Grade Threshold (MGT) example

of the node between the two positions in the two beacons exceeds the MGT. If so, the sending node is rated accordingly in the trust model.

A potential motivation for the MGT sensor is demonstrated in Figure 4. We assume that a rational attacker A (again located at position A_r) promiscuously listens the communication channel for packets he would like to intercept. If node M forwards packet P_1 to node N, A receives it as well, but cannot prevent further forwarding, because A is not in the route. However, A may instantly send a beacon with a virtual position A_{v1} that N will likely select as next forwarder for P_1. The only constraint is to be faster than the forwarding process at N. A similar kind of attack has already been introduced for topology-based routing protocols in [22]. Using this method, A is able to intercept all nearby packets assuming it is capable of taking in new positions as often as required. For example, shortly after setting its position to A_{v1}, A may set it to A_{v2} in order to intercept another packet P_2. This uncontrolled position hopping is detected by the MGT sensor.

However, whereas the sensor detects rapid changes in a node's alleged position, it cannot detect gradual changes of a node's position claim towards a wrong direction.

3) Maximum Density Threshold: Similar to the last sensor, this sensor is based on the assumption that only a restricted number of physical entities (e.g. cars) can reside in a certain area. For example, cars have certain physical dimensions preventing too many of them to be on the same road segment.

This sensor defines a Maximum Density Threshold (MDT) which, when exceeded, rejects further position beacons for this area. It aims at preventing so called Sybil attacks, where a node creates a large number of virtual nodes in order to collect all traffic in a certain area [23]. Additionally, vehicle speed could be taken into consideration because higher vehicle speeds usually result in lower node densities.

4) Map-based Verification: Here, we assume that cars include navigation systems where street maps are accessible by the position verification system. Upon receiving a beacon, the system can check whether a neighboring car pretends to be at a location that is not likely, e.g. off the streets, in houses, etc.

Map-based verification reduces the set of valid positions and serves for instance to detect faulty operation of an others vehicles' positioning system, that is continuously broadcasting off-road positions in its beacon messages.

5) Position Claim Overhearing: Overhearing is a concept introduced by Marti et al. [24] where nodes use the so-called promiscuous mode to capture packets that are sent by nodes in reception range but are addressed to other nodes. Whereas Marti et al. use this concept to detect packet dropping and to control forwarding behavior of nodes, we use it to verify position information. As shown in Figure 5, there are two cases where overhearing is useful (again, A_r represents the real position of node A, whereas A_v denotes the position, A pretends to be in its beacon messages).

In the first case, node M forwards packet P_1 to node A. Later M overhears P_1 being sent to node L which is at an inferior position (with regard to the routing metric) compared to A. This indicates that A may have forged its position A_v. In the second case, node M overhears the transmission of packet P_2 from N to A, although given the last position of A known to M and the Mobility Grade Threshold, A should not be in reach of N. Again this indicates that A may have forged its position A_v.

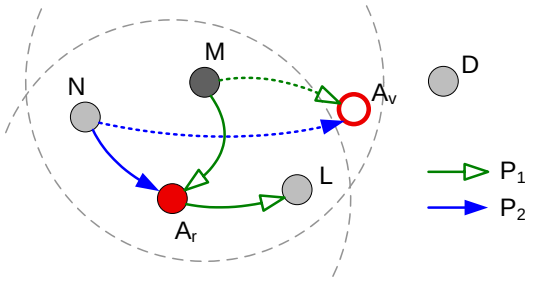

Fig. 5. Position Claim Overhearing example

Whereas the earlier sensors are quite reliable, the overhearing sensor gives only indications that position information may have been forged. There are valid cases where the overhearing sensor will wrongly detect nodes to spoof positions. So the overhearing sensor should only be used in combination with other sensors.

C. Cooperative Sensors

1) Proactive Exchange of Neighbor Tables: Here nodes exchange their neighbor tables and then check if the positions received correspond to their own data. One can further distinguish whether the exchanged neighbor tables include the position of neighbors or only the fact that two nodes share a common link.

In the first case, when a node N receives a beacon from node M claiming to be at position P_B and receives a neighbor table from node O containing the information that M is at position P_B and P_B and P_B differ significantly (taking into account the time difference between the two measurements), N can conclude that one of the position claims must be false. In this case it cannot determine if M is sending false information or whether O has modified the information in its neighbor table. When more neighbors distribute their neighbor tables, N can take a majority decision whether to believe the position claim of M or not.

If O sends the neighbor table without position information, N can apply a verification mechanisms similar to the ART sensor to check if M at its claimed position P_B is in the range of O – then it must appear in the neighbor table of O – or if M is outside of the transmission range of O – in this case M must not appear in the neighbor table of O.

Of course these checks have only statistical significance and thresholds must be applied to prevent too many false-positives. Further the results are not taken directly as a base for the decision which position information to drop, but are combined with other observations as described in section IV-A. So only the combination of multiple observations lead to the rejection of a position claim.

2) Reactive Position Requests: For this sensor, nodes only cooperate for position verification upon demand. This could be triggered when a node N encounters an other node M which it has never met before. This is step 1 in the example in Figure 6. Besides, the necessity to verify position claims of an already known neighbor could be raised by indications from autonomous sensors, which indicate that the node has started to cheat about its position.

Thus, the corresponding node N starts the verification process by selecting several neighbors as acceptor or as rejector. Because N knows the positions of its own neighbors, the claimed position of M as well as the theoretical transmission range of the radio hardware, N is able to distinguish between own neighbors that should have received beacon messages of M and those that should have missed beacons because their distance to M is too large. Hence, it randomly selects some rejectors among those neighbors that should not have received a beacon from M and some acceptors from those that are supposed to have received one. Having recorded this, N sends out a position request (PREQ) in which all acceptors and rejectors are asked for the position of M (step 2 in Figure 6). In case an addressed node does not know M yet, it needs to answer as well with an according message (step 3).

After having received the responses, N is able to compare them with what it expected and can rate the position claim of M. For instance, the more supposed rejectors actually got the current beacon from M,

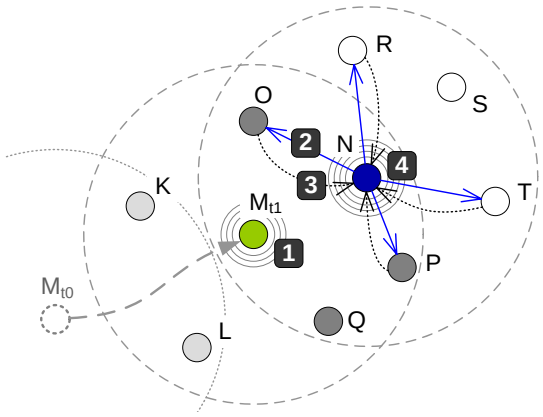

Fig. 6. Reactive Position Request example

	Communication overhead	Suitability for high mobility	Robustness against attacks	Robustness against exploits	Verification performance
ART	++	++			+
MGT	++	++			○
MDT	++	+			-
Overhearing	++	○			○
Map-based verification	++	++			+
Proactive neighbor exchange					
- including positions	– –	–	○	– –	++
- without positions	–	–	○	–	+
Reactive position requests	○	○	+	+	+

TABLE I
COMPARISON OF THE PROPOSED SENSORS FOR THE TRUST SYSTEM

the lower the sensor output will be, because this indicates that M has given a falsified position. Finally, N optionally distributes the result of the verification to its neighbors (step 4).

D. Comparison of Different Sensors

As explained in the previous sections, every sensor targets a specific constraint that indicates a position falsification. For instance, the ART sensor will obviously only be able to detect fake positions outside of the radio range of the receiving node. Or, the MGT sensor will only detect ”position hopping”, not the slow continuously displacement of a fake position. Therefore, every sensor has its particular advantages and disadvantages in its contribution to the verification system. In Table I, we compare the presented sensors according to qualitative criteria.

When we look at the two different classes of sensors, autonomous sensors have the advantage that they do not require additional communication between the nodes. Furthermore, they also work reliable in sparse networks and they are not influenced by message loss.

Cooperative sensors obviously require a certain number of neighboring nodes. The key advantage of cooperative sensors is adaptivity to the current situation and a higher accuracy due to different points of view of different nodes. Thus, cooperative sensors can deliver a higher accuracy for the position verification. The downside of cooperative sensors is that they need to communicate and exchange information in

Parameter	Urban areas	Motorway
Number of nodes	100	100–1000
Field	1000–4000m square	12km, 2 lanes per direction
Node density	100–6,25 nodes/km^2	$\sim$ 6 nodes/km/lane
Avg. node velocity (m/s)	25	40
Pause times (s)	0.0	
Mobility model	Random Waypoint	Driving simulator based
Link-/MAC-Layer	IEEE 802.11	
Transmission range (m)	250	
Number of sent messages	100	
Simulation time (s)	60	
Simulation runs	20	

TABLE II
SHORT OVERVIEW ON SIMULATION PARAMETERS

order to detect position faking nodes. However, the resulting communication overhead could be limited by using such sensors selectively, e.g. only when autonomous sensors indicate that position faking may be going on. It is also important to note that the cooperative mechanisms – if not secured properly – may create additional attack opportunities. Position faking nodes could send wrong information messages to it's neighborhood or extract information from the exchanged packets to even improve their position faking. The influence of message loss on cooperative sensors is limited; if verification data is lost this results in no rating.

The comparison of autonomous sensors amongst each others regarding the qualitative criteria in Table I reflects only minor differences. Overhearing and MDT are less suitable for high mobility scenarios since they require a slightly more stable network topology to produce stable results. The verification performance of MGT, MDT and Overhearing is lower since the sensors produce less accurate results.

The comparison of cooperative sensors mainly shows the trade of between communication overhead and verification performance. Proactive exchange requires more communication and is thus also more prone to abuse by an attacker, But, it results in higher verification performance.

V. ANALYSIS

A. Simulation Environment

For the purpose of evaluation of the presented verification techniques, we implemented them in the ns-2 network simulator (ns-2.27). Our simulation environment consists of the following key components

- Routing, namely geographic with caching (CGGC)
- Data traffic and node mobility model
- Attacker model
- Verification system with ART, MGT and reactive position requests as input sensors

These components are explained in detail in the following.

1) Geographic Routing: For the simulations, we used a greedy based routing approach, which selects the neighbor closest to the destination as next hop for a packet. In case that no suitable next hop is available when a packet has to be forwarded, the recovery strategy is based on caching, i.e. packets are stored locally until either a suitable neighbor is reachable or until the node is forced to drop the packet due to packet queue overflow. Details of this geographic routing approach have been studied in (see [9].

2) Node Mobility and Data Traffic Scenario: The simulation scenario has to consider mainly two parameters, data traffic and node mobility. As data traffic, 100 messages are transmitted from a random source node to a random destination node. Those messages are created between simulation time $t = 0s$ and $t = 30s$.

Concerning node mobility in VANETs, we distinguish between urban areas and rural roads or highways. Whereas urban traffic is rather complex and undirected, the movements on roads outside of cities like

on highways or on freeways can be considered nearly one-dimensional. In [25], the authors have found that urban traffic can be modeled with random waypoint movements, therefore this model is at least appropriate for simulating VANETs in cities. For non-urban roads, we conducted simulations using traffic scenes from a Daimler driver behavior simulator called FARSI that gives realistic vehicle movements on a multi lane motorway. Further simulation parameters are listed in Table II.

3) Attacker Model: Maliciously acting nodes are implemented according to the following model. Whenever a malicious node is about to send a beacon message to announce its present position, it selects a random position on the field and applies it to the beacon instead of its actual position. For the highway scenario, we implemented also the special case of a more intelligent acting single stationary attacker. He distributes beacons with two different position informations. These two position informations are symmetrically aligned to its actual position in both directions of the highway.

The second parameter of the attacker model is the forwarding behavior of the attacker. Whenever a malicious node gets a data packet, depending on the simulation setup, it either forwards it correctly according to the protocol rules or it drops the packet.

In other words, falsifying the position is the method to intercept or reroute packets which then may be examined and forwarded for eavesdropping reasons or even be dropped to disconnect routes.

4) Verification System: The trust system is implemented to be used in all nodes. It assigns trust levels to a node's direct neighbors according to the observations of different sensors. The initial trust value for a previously unknown neighbor node is neutral (i.e. 0). As mentioned in the description of the trust system, every sensor gets an individual weight that reflects the reliability of the sensor. During our simulations, we assigned the ART sensor a weight of 5 and the MGT sensor a weight of 3. As cooperative method, the reactive position request was implemented and weighted using the number of responses to a position request. Autonomous sensors get active for every received beacon message, whereas the cooperative check is only done when either a new node is encountered, or a node is suspicious for having started to spoof its location. Depending on the results of the sensors, the trust level of the corresponding neighbor is either increased or decreased.

The collected trust levels are finally applied in the forwarding process. As candidates for the next hop of a packet, only nodes with a positive trust level (i.e. $[0; 1]$) are considered, whereas nodes with a negative level (i.e. $[-1; 0)$) are disregarded.

The following sections will discuss our simulation results and evaluate the detection capabilities of our decentralized position verification system.

B. Detection Quality Analysis

The effectiveness of the position verification system can be assessed both, with external indicators as well as with internal results (internal indicators) of the trust system. External indicators are values reflecting the activity of the trust system, for instance, the average delivery ratio of the system, or the number of forwarded packets by malicious nodes. While these values indirectly reflect the operation of the trust system, we are also able to directly monitor the trust levels that are assigned to malicious nodes by ordinary nodes throughout the simulation run. In this case, we obtain a more direct evaluation of the trust system.

Our previous work with autonomous sensors only has shown that the simulation results in city scenarios and highway scenarios are similar. In some cases, attackers have a higher influence in highway scenarios due to the quasi linear node distribution. Consequently, in this analysis we focus on selected simulation results from both scenarios to provide an overall analysis of the combined verification system.

1) External Indicators: Figure 7a shows the successfully delivered messages in dependence of the network size in a city scenario. Note that varying the network size while keeping the number of nodes constant is equivalent to varying the node density. We observe that the number of successfully delivered messages is decreased significantly when position-faking nodes also drop received messages immediately. To let malicious nodes drop packets is an appropriate way to get an estimation on the number of intercepted messages by these nodes.

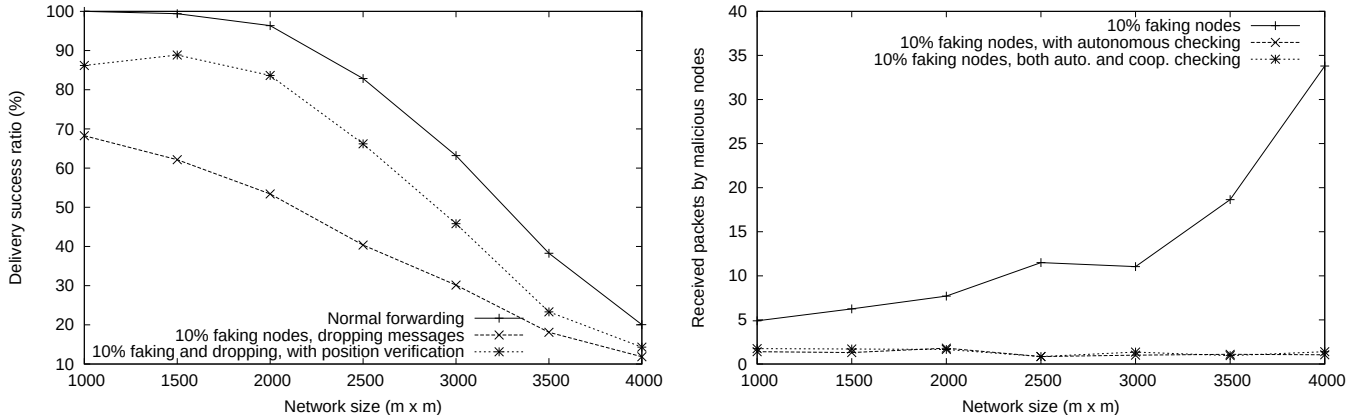

Fig. 7. a) Delivery success ratio (city scenario) and b) intercepted packets with application of the position verification system (city scenario)

With the trust system applied, the position faking nodes are detected by normal nodes and therefore are no longer selected as forwarders for packets. The result is an increased rate of successfully delivered messages. However, the use of the trust system cannot reach the delivery ratio without malicious nodes since the effective node density is also decreased when malicious nodes are excluded from the forwarding process.

The same observations can also be seen in Figure 7b, where we depict the average number of messages that a malicious node has received. When normal nodes detect a cheating node, they should refrain from using it as a packet forwarder. Therefore, such nodes should no longer receive packets in the optimum case. In fact, we see that this number reduces nearly to zero when the verification system is applied, thus we effectively excluded malicious nodes, of course to the cost of lower network density. Figure 7b shows also that in the case of a randomly position faking attacker, there is no benefit of cooperative mechanisms. The autonomous sensors provide sufficient detection. The reason is that in most cases the position information distributed by the attacker exceeds the acceptance range threshold of the ART sensor. The benefit of cooperative mechanisms over autonomous mechanism will be analyzed more detailed with the internal indicators.

2) Internal Indicators: As important internal measures of the verification system, we consider the detection rate and the false positives in Figure 8 The detection rate is given by the ratio of successfully identified position faking nodes vs. the total number of position fakers. In contrast, false positives describe the incorrect accusations.

With regard to these indicators, we can explain the observations from the indirect measurements like delivery success ratio. Figure 8a shows the detection rate in a highway scenario with the stationary attacker as introduced above. The detection rate is shown in dependence of the distance between the attackers real position and the position information, which is distributed in the beacon information. We see that the combination of autonomous and cooperative sensors reaches a detection rate from 90% to even over 95%. When we look at the results of autonmous sensor in the case of small distances between actual and claimed position, this figure clearly shows the main advantage of cooperative sensors. Whereas the verification system reaches only moderate results when only autonomous sensors are used, cooperative sensors can deal very well with small distances between actual and claimed position.

Another relevant internal measurement are false positives, which represent the amount of erroneous detections. Figure 8b shows the false positives with different sensors applied in a city scenario. Again, we analyze false positives in dependence of the network size, which is equivalent to the node density. Here, we observe a higher rate of wrong detections when the cooperative sensor is included in the position verification. In the current setup, the cooperative sensors tend to achieve higher detection accuracy to the cost of higher false positives. However, the rate is still at an acceptable level. For both types of sensors, the increased rate of false positives in less dense scenarios is the natural result of the very unstable network

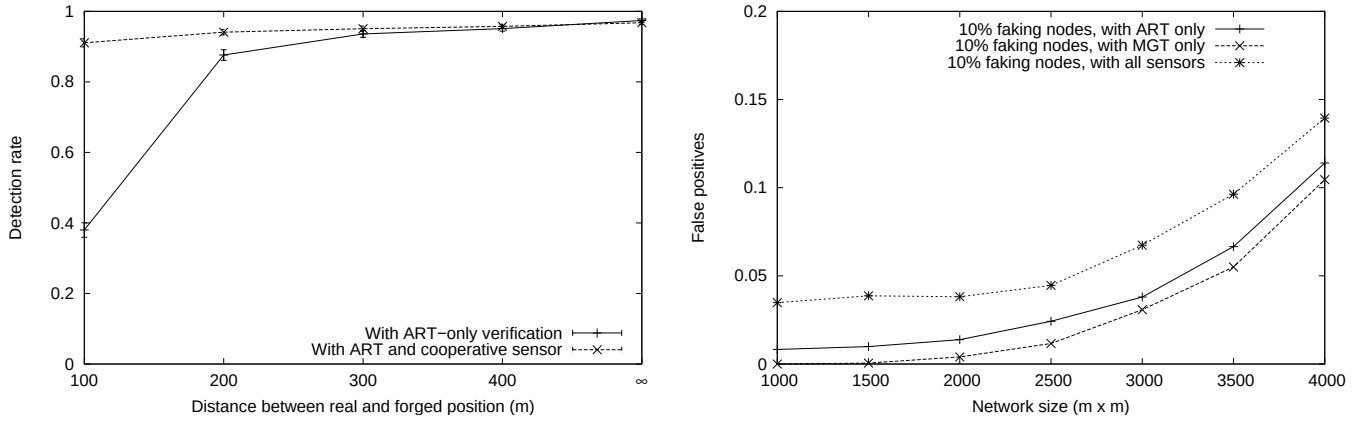

Fig. 8. a) Detection rate (highway scenario) and b) false positives of the verification system (city scenario)

topology.

C. Weaknesses and Attacks

When analyzing our position verification system, we found that there are some weaknesses that might be improved in future versions. Consequently a smart attacker might find ways to fool the verification system.

One drawback of our current solution is that we use only hard thresholds. While the applied thresholds were found in simulations to be suitable for most scenarios, in reality there will be conditions where the thresholds are not strict enough. For instance, think of ART, which limits the maximum range of signals. If we choose the ART value for a general scenario, we need to set it to the maximum communication range of the radio technology used in a free open space. For IEEE 802.11 WLAN, $300m$ should be a reasonable value. But if the same technology is used e.g. in a narrow city center where a lot of buildings would block the signals, the same $300m$ might never be reached in reality. Allowing spoofed positions $300m$ away from the correct position might then be enough for reaching the attackers goal, e.g. capturing traffic etc. as all the other nodes available for forwarding are much nearer.

A solution to that problem is to choose adaptive thresholds, that are set according to the location conditions. If for example all neighbors are within $50m$ range, a node being away $150m$ might be more suspicious as in a setting where also other nodes are 100 to $150m$ away. This can be expressed by varying the sensor rating σ_n^s between the allowed range of $+1$ and -1. In the first case the rating might be set to -0.5 whereas in the second case a rating of $+0.5$ could be appropriate.

Another area for improvements might be the forwarding decision. Currently, nodes with negative rating are not used for forwarding. One might make a finer distinction where there are groups of nodes that have e.g. ”no trustworthiness”, ”limited trustworthiness” and ”full trustworthiness”. In the trust system, this might correspond to ratings ranging from $[-1; -\frac{1}{3})$, $[-\frac{1}{3}; \frac{1}{3})$, and $[\frac{1}{3}; 1]$. In such a setting, only fully trustworthy nodes are chosen in all forwarding decisions. If no such nodes are available, nodes with limited trustworthiness can be selected as an alternative, whereas not trustworthy nodes are never used. This could help improve the packet delivery ratio in networks with low node density.

We assume that all details of the verification system are also known to a potential attacker that might try to misuse the system for attacks.

A straightforward attack would be the dissemination of spoofed beacons to reduce the rating of other nodes. Such an attack can also be an effective DoS attack in VANETs without position verification system. This could be prevented by authenticating position beacons. Beacon authentication can be achieved by signatures or more advanced schemes that are e.g. based on MACs or hash-chains.

If the ART is known, malicious nodes may decide to avoid the position verification system by staying just within the ART. As already explained, depending on the distribution of nodes and the reception

conditions, this may allow malicious nodes to capture traffic. In fact, this is what is shown in Figure 8a, where the ART sensor performs poorly with low distances between real and forged positions. But this figure also shows already a possibility to defend against such malicious nodes, namely the usage of cooperative sensors. Another solution that mitigates this attack is the use of adaptive thresholds as outlined above. One might also correlate the claimed position with the received signal strength indicator that most radio technologies provide. This way unreasonable position claims within the ART range may also be identified.

As mentioned earlier, the MGT might be fooled by slowly changing the pretended position towards a destination without exceeding maximum mobility grade. There is no way to detect this kind of behavior with the MGT sensor. However, as we assume additional sensors like ART to be in place, the effects of this attack are limited.

The MDT sensor might be attacked by creating faked nodes within a target area thus exceeding the MDT limit. Normal nodes in the same area could get assigned bad ratings by surrounding nodes. A potential solution would be to require beacons to be authorized by a trusted third party (e.g. signed with a certificate). Under this assumption, a node can only fake one position per time. However, requiring beacons to be authenticated has large impact on node privacy and required infrastructure, which is out of scope for this paper.

The overhearing sensor might also be the goal of an attack. As overhearing is in general very inaccurate, this should only be used as trigger for other (e.g. cooperative) sensors. This way the effects of attacking overhearing are limited.

Regarding the cooperative sensors, two facets need consideration. On the one hand, the verification process itself may be subject to attacks, and on the other hand, the mechanism may introduce new starting points for other attacks.

For instance, in the case of reactive position requests, it is possible that an arbitrary node M answers the position request on behalf of an actually questioned node Q. However, as such a node M does not know if the requesting node R regards a questioned node Q as rejector or acceptor, it still might not profit. As solution to the problem, the nodes might pairwise exchange keys when they encounter each other (Diffie-Hellman key exchange) and use these keys subsequently when sending the response to the requesting node R.

In the second case, an attacker might abuse the communication process, e.g. by continuously sending out position requests and have lots of other nodes answer to these requests. Thus, an attacker could consume considerable channel capacity. However, as the requested nodes are around the attacker, it will also suffer from that effect and it won't be able to use the bandwidth.

VI. Conclusions

Falsified position information in mobile ad hoc networks with geographic routing protocols results in serious network performance degradation. This paper briefly summarized our previous analysis of local and global effects of falsified position information [10], [11].

We have developed mechanisms to detect and mitigate the influence of falsified position information in geographic routing protocols. In contrast to other position verification approaches, we do not rely on special hardware to measure signal strengths or time-of-flight, nor do we rely on a preinstalled infrastructure networks. In order to improve reliability of position information, our goal is to quickly estimate the trustworthiness of the position claims of neighbored nodes.

The selected mechanisms will not prevent malicious nodes entirely from using falsified position information, however, they will drastically limit the choice of fake positions that will not be detected by our system (i.e. fake positions must meet all criteria as opposed by the deployed sensors, for instance they must reside within a node's wireless transmission range). Consequently the possibilities for attackers using faked positions are significantly reduced.

We discussed advantages and drawbacks, respectively vulnerabilities of our detection techniques. We have presented performance measurements for autonomous and cooperative sensors. They indicate that

cooperative sensors increase the detection capabilities of the verification system, especially in case an attacker circumvents the otherwise reliable acceptance range threshold (ART) sensor (i.e. the attacker choses a small distance between his real and his forged position). However, the cooperative sensors come with the disadvantages of communication overhead and of a slightly increased rate of false positives.

In future work, we plan to tune the sensor setup of the cooperative sensor in order to reduce the number of false positives. We will also compare in more detail the detection rates of autonomous and cooperative sensors in different scenarios with different node densities and different types of attackers.

REFERENCES

[1] W. Franz, C. Wagner, C. Maihöfer, and H. Hartenstein, "FleetNet: Platform for Inter-Vehicle Communications," in *Procedings of 1st International Workshop on Intelligent Transportatin (WIT'04)*, Hamburg, Germany, Mar. 2004.

[2] CarTalk 2000, "CarTalk 2000," http://www.cartalk2000.net, 2004.

[3] VSCC, "US Vehicle Safety Communication Consortium," http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm.

[4] C2C-CC, "Car2Car Communication Consortium," http://www.car-to-car.org/.

[5] NoW, "Network on Wheels," http://www.network-on-wheels.de, 2005.

[6] Holger Füssler, Martin Mauve, Hannes Hartenstein, Michael Käsemann, and Dieter Vollmer, "A Comparison of Routing Strategies for Vehicular Ad Hoc Networks," Technical Report TR-3-2002, Department of Computer Science, University of Mannheim, July 2002.

[7] David B. Johnson, David A. Maltz, and Josh Broch, *DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks*, chapter Chapter 5, pp. 139–172, Addison-Wesley, 2001.

[8] Charles E. Perkins and Elizabeth M. Royer, "Ad hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, February 1999, pp. 90–100.

[9] Christian Maihöfer, Reinhold Eberhardt, and Elmar Schoch, "CGGC: Cached Greedy Geocast," in *Proceedings of 2nd Intl. Conference Wired/Wireless Internet Communications (WWIC 2004)*, Frankfurt (Oder), Germany, Feb. 2004, vol. 2957 of *Lecture Notes in Computer Science*, Springer Verlag.

[10] Tim Leinmüller, Elmar Schoch, Frank Kargl, and Christian Maihöfer, "Influence of Falsified Position Data on Geographic Ad-Hoc Routing," in *Proceedings of the second European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2005)*, July 2005.

[11] Tim Leinmüller and Elmar Schoch, "Greedy routing in highway scenarios: The impact of position faking nodes," in *Proceedings of Workshop On Intelligent Transportation (WIT 2006)*, Mar. 2006.

[12] Tim Leinmüller, Elmar Schoch, and Frank 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.

[13] Tim Leinmüller, Elmar Schoch, Frank Kargl, and Christian Maihöfer, "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*, New York, NY, USA, 2006, pp. 57–66, ACM Press.

[14] Frank Kargl, Stefan Schlott, Michael Weber, Andreas Klenk, and Alfred Geiß, "Securing Ad hoc Routing Protocols," in *Proceedings of 30th Euromicro Conference*, Rennes, France, Aug. 2004.

[15] Frank Kargl, Alfred Geiß, Stefan Schlott, and Michael Weber, "Secure Dynamic Source Routing," in *Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS-38)*, Hilton Waikoloa Village, HA, Jan. 2005.

[16] Jean-Pierre Hubaux, Srdjan Čapkun, and Jun Luo, "The Security and Privacy of Smart Vehicles," *IEEE Security and Privacy*, vol. 4, no. 3, pp. 49–55, 2004.

[17] Srdjan Čapkun, Levente Buttyán, and Jean-Pierre Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN 2003)*. 2003, pp. 21–32, ACM Press.

[18] Naveen Sastry, Umesh Shankar, and David Wagner, "Secure verification of location claims," in *Proceedings of the 2003 ACM workshop on Wireless security (WiSe'03)*. 2003, pp. 1–10, ACM Press.

[19] Adnan Vora and Mikhail Nesterenko, "Secure location verification using radio broadcast," in *Proceedings of 8th International Conference on Principles of Distributed Systems (OPODIS 2004)*. 2004, Springer Verlag.

[20] Frank Kargl, Andreas Klenk, Stefan Schlott, and Michael Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks," in *Proceedings of 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*. Sept. 2004, pp. 152–165, Springer Verlag.

[21] Pietro Michiardi and Refik Molva, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, Deventer, The Netherlands, The Netherlands, 2002, pp. 107–121, Kluwer, B.V.

[22] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the ACM Workshop on Wireless security (WISE)*, San Diego, CA, USA, 2003, pp. 30–40.

[23] James Newsome, Runting Shi, Dawn Song, and Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," in *Proceedings of IEEE International Conference on Information Processing in Sensor Networks (IPSN 2004)*, Apr. 2004.

[24] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 255–265.

[25] Amit Kumar Saha and David B. Johnson, "Modeling mobility for vehicular ad-hoc networks," in *Proceedings of the first ACM workshop on Vehicular ad hoc networks (VANET '04)*. 2004, pp. 91–92, ACM Press.