

# Secure Position-Based Routing for VANETs

Charles Harsch<sup>1,2</sup>, Andreas Festag<sup>1</sup>, Panos Papadimitratos<sup>2</sup>

<sup>1</sup> NEC Deutschland GmbH, {harsch|festag}@netlab.nec.de

<sup>2</sup> EPFL, Switzerland, {charles.harsch|panos.papadimitratos}@epfl.ch

**Abstract**—Vehicular communication (VC) systems have the potential to improve road safety and driving comfort. Nevertheless, securing the operation is a prerequisite for deployment. So far, the security of VC applications has mostly drawn the attention of research efforts, while comprehensive solutions to protect the network operation have not been developed. In this paper, we address this problem: we provide a scheme that secures geographic position-based routing, which has been widely accepted as the appropriate one for VC. Moreover, we focus on the scheme currently chosen and evaluated in the *Car2Car Communication Consortium (C2C-CC)*. We integrate security mechanisms to protect the position-based routing functionality and services (beaconing, multi-hop forwarding, and geo-location discovery), and enhance the network robustness. We propose defense mechanisms, relying both on cryptographic primitives and plausibility checks mitigating false position injection. Our implementation and initial measurements show that the security overhead is low and the proposed scheme deployable.<sup>1</sup>

## I. INTRODUCTION

In the near future, vehicles will be equipped with wireless communication devices, allowing for vehicle-to-vehicle and vehicle-to-infrastructure communication based on short-range wireless technology (IEEE 802.11-like). These vehicular ad hoc networks (VANETs) enable a new set of applications to improve safety, traffic efficiency and driving comfort. For example, a vehicle can warn other vehicles about traffic accidents or bad road conditions.

The specific conditions and requirements for vehicular communication (frequent topology changes, short connectivity times, and the positioning system GPS) have justified the development of a dedicated routing solution for wireless multi-hop communication based on geographic positions [1], [2], [3]. Position-based routing (PBR) provides scalable and efficient (unicast) forwarding in large-scale and highly volatile ad hoc networks, in contrast to topology-based ad hoc routing. PBR is currently considered and evaluated by the *Car2Car Communication Consortium (C2C-CC)*.<sup>2</sup> PBR, described in further detail in Sec. II, basically comprises a location service that maps a given node ID to its current position, geographic unicast communication, and distribution of packets in geographic areas. These services, in addition to single-hop broadcast, enable road safety applications that disseminate safety information either as 'event-driven messages' (e.g. de-centralized

hazard warning) or 'periodically-sent beacons' (e.g. extended electronic break-light, forward collision warning). PBR also provides packet transport for vehicle-to-vehicle and vehicle-to-roadside communication for non-safety applications.

It is vital to secure communication in VANETs, otherwise the benefits of those novel networks can turn into a nightmare: an attacker could send falsified information to other nodes, or block others from receiving safety messages. Since periodic safety messages are single-hop broadcasts, the focus has been mostly on securing the application layer. For example, the IEEE P1609.2 draft standard [4] does not consider the protection of multi-hop routing. However, when the network operation is not secured, an attacker could easily partition the network and make delivery of event-driven safety messages impossible. For example, the attacker could advertise a lot of falsified identity/position pairs to its neighbors, thus forcing them to believe there are many neighbors. It is highly probable packets are lost when forwarded to non-existent nodes.

In this paper, we address the security of the network layer operation for wireless multi-hop communication in VANETs. We analyze vulnerabilities and potential attacks against geographic routing, and in particular the considered PBR. Based on the analysis, we design a security scheme that protects the PBR services, such as the exchange of nodes coordinates, multi-hop (unicast and broadcast) communication, and the correctness of the location service.

Previous work has presented design principles [5], [6], attacks [7], [8], and components of a secure VANET architecture [9], [5]. Only a few works consider security of geographic routing: [10], [11], [12] focus on plausibility checks for received location beacons, while [13] proposes a secure grid based location service, secure broadcast authentication for hop-by-hop protection, and a reputation system. Compared to [13], our work targets the highly volatile, large-scale VC environment that would make symmetric key mechanisms and reputation systems hard to implement. Our focus is on communication and networking, and is orthogonal to the location service described in [13]. Also, our work is complementary to [10], [11], [12], since it provides a comprehensive security solution and it is tailored to the specific PBR protocol.

In the rest of the paper, we first explain the basics of PBR in Sec. II. Then, the security objectives are listed in Sec. III, with Sec. IV discussing an adversary model and attacks on PBR. Sec. V presents the proposed scheme, Sec. VI analyzes its properties and reports initial implementation measurements, before we conclude.

<sup>1</sup>C. Harsch and A. Festag acknowledge the support of the German Ministry of Education and Research (BMB+F) for the project 'NoW – Network on Wheels' under contract number 01AK064F.

<sup>2</sup>The C2C-CC is an industry consortium that develops a standard for vehicular communication based on IEEE 802.11 technology. <http://www.car-to-car.org>

## II. POSITION-BASED ROUTING PROTOCOL

Position-based routing provides multi-hop communication in a wireless ad hoc network. It assumes that every node knows its geographic position, e.g. by GPS, and maintains a location table with ID and geographic positions of other nodes as soft state. PBR supports *geographic unicast* (GeoUnicast), *topologically-scoped broadcast* (TSB, flooding from source to nodes in n-hop neighborhood), *geographically-scoped broadcast* (GeoBroadcast, packet transport from source to all nodes in a geographic area) and *geographically-scoped anycast* (same as GeoBroadcast, but to one of the nodes in the area). Basically, PBR comprises three core components: beaconing, a location service, and forwarding.

**Beaconing:** Nodes periodically broadcast short packets with their ID and current geographic position. On reception of a beacon, a node stores the information in its location table.

**Location Service:** When a node needs to know the position of another node currently not available in its location table, it issues a *location query* message with the sought node ID, sequence number and hop limit. Neighboring nodes rebroadcast this message until it reaches the sought node (or the hop limit). If the request is not a duplicate, the sought node answers with a *location reply* message carrying its current position and timestamp. On reception of the *location reply*, the originating node updates its location table.

**Geographic Unicast** provides packet transport between two nodes via multiple wireless hops. When a node wishes to send a unicast packet, it first determines the destination position (by location table look-up or the location service). Then, it executes a *greedy forwarding* algorithm, sending the packet to its neighbor with the minimum remaining distance to the destination (most-forward-within-radius strategy [14]). The algorithm is executed at every node along the forwarding path until the packet reaches the destination.

**Geographic Broadcast** distributes data packets by flooding, where nodes re-broadcast the packets if they are located in the geographic area determined by the packet. Also, advanced broadcasting algorithms ensure avoidance of the so-called 'broadcast storms' minimize overhead.

A number of mechanisms enhance the basic forwarding schemes: if a forwarder has more recent (up-to-date) information in its location table about a given destination, it updates on-the-fly the destination position and timestamp values in the packet header. Similarly, based on received packet headers with newer information, nodes update its location table.

PBR defines packet headers with fields for node ID, position and timestamp for a source, sender, and destination, and others.<sup>3</sup> For GeoBroadcast, the header carries a destination area instead of a destination ID. For the header fields we distinguish between immutable and mutable fields. *Immutable* fields are not altered during forwarding, whereas *mutable fields* can be updated by forwarders (see the example GeoBroadcast header in Fig. 1).

Packet Type	Subtype	TTL	Flags
Length		Protocol	Priority
Sequence Number		Source Timestamp	
Source ID			
Source Position (Latitude/Longitude)			
Sender ID			
Sender Position (Latitude/Longitude)			
Sender Timestamp		Target Area Class	
Target Area Position 1 (Latitude/Longitude)			
Target Area Position 2 (Latitude/Longitude)			
Target Area Size			

Immutable Fields  
(dark)

Mutable Fields  
(light)

Fig. 1. Example packet type with mutable and immutable fields

## III. SECURITY OBJECTIVES

Since forwarding is based on position information, location information obtained by correct nodes must correspond to *plausible* node positions. That is, positions within a degree of accuracy from the *actual* node positions. Plausibility of location information, rather than actual locations, allows to account for system volatility and realistic limitations, as it will be explained in Sec.VI.

Location information, e.g., in the *location table*, is deemed *plausible* with respect to the reported time, location and the node's own data. It is evaluated based on the received message reporting the location, e.g., beacons or *location service* replies. In both cases, *authentic* reporting of position information must be ensured. Nodes are solely responsible for providing their location information and impersonation must be impossible.

Data and control packet *forwarding* must be *loop-free* and *towards the destination* or target area location.<sup>4</sup> Having packets forwarded across the shortest path towards the destination is not a requirement due to the high network volatility.

The system should be *robust* against abuse of the position-based communication services, in particular towards resource depletion. Abuses beyond the PBR functionality (e.g., data link or physical layer jamming) are out of scope.

The above PBR-specific requirements can be related to traditional security requirements. *Authentication*, and the resultant *integrity* and *non-repudiation* of packets (e.g., beacons and location queries and replies) can be sought as the means to prevent impersonation and other manipulation of location information. Or, facilitate forwarding towards the destination, by preventing alteration of this information in packets. *Freshness* can be the means to verify plausibility, e.g., by preventing replayed location information. *Authorization* can assist the robustness, allowing nodes to utilize resources (e.g., initiating geo-broadcasts) according to their assigned roles in the system.

Authenticity, non-repudiation and integrity are required for PBR control packets and fields. It is thus straightforward to require them for data (i.e., payloads) as well. *Reliability*, however, is not a direct requirement at this stage, as communication is not two-way. In the case of broadcast or flooding, reliability is inherent. Redundant forwarding could also assist towards reliability for unicast. *Privacy* is not a requirement

<sup>3</sup>The originator of a message is referred to as source, and the last forwarder as sender.

<sup>4</sup>Unless the packet is cached or re-routed across an alternative route segment, to bridge or circumvent "gaps" due to greedy forwarding.

either, and it is largely orthogonal to our scheme. The selection of a privacy enhancing solution could nonetheless affect the network performance; for the case of frequent pseudonym changes we refer to [15], [16].

#### IV. ATTACKS

An extensive study on different adversary models has been presented in [5]. Here, we describe attacks relevant to position-based routing, to guide the design of security countermeasures. Attack trees [17] provide a standardized method to classify attacks on a system: the root represents a general attack further refined in the tree structure using *AND* and *OR* logical connections. The complete attack tree analysis is out-of-scope of this paper, but it is available in [18]. A simplified version of the sub-tree on denial of service attacks against PBR is shown in Fig. 2, and detail some abuses.

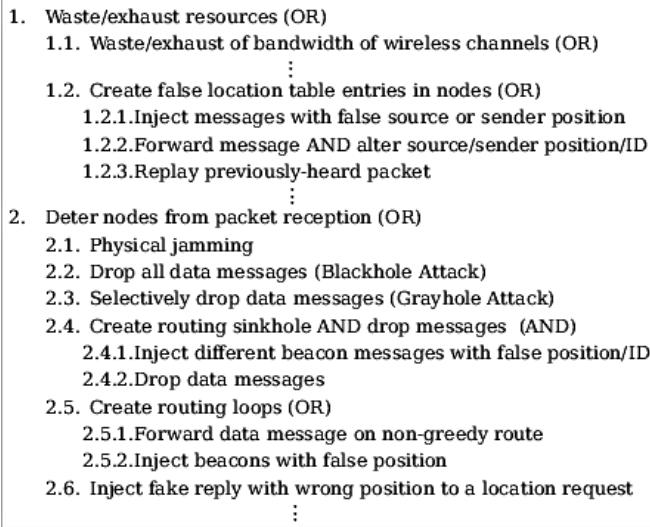


Fig. 2. Simplified DoS-against-PBR attack sub-tree

- *False Position Advertisement*: The attacker claims to be at a different position than its actual one, e.g., by including it in a beacon, data packet, or a location reply.
- *Geographic Sybil Attack*: The attacker advertises multiple IDs and/or positions, to mislead other nodes that high numbers of (non-existent) neighbors exist. Communication across non-existing nodes is in full control of the attacker; e.g., forwarded packets will be lost.
- *Packet Alteration*: An attacker changes, in an unauthorized manner, the content of the header or payload of the packet it forwards. The former can poison the location table of subsequent forwarders.
- *Packet Dropping*: Attackers selected as forwarders can simply drop packets, either all (*black-hole attack*) or selectively (*gray-hole attack*).
- *Replay*: The attacker re-injects previously received packets into the network. For example, the attacker can poison a node's location table by replaying beacons.
- *Packet Injection*: Attackers transmit location queries or geo-broadcast (or even unicast) packets at high-rates, to

consume bandwidth and computation power in large parts of the network.

#### V. SECURE PBR

We design mechanisms to safeguard the functionality of PBR, relying both on cryptographic primitives and plausibility checks, towards achieving the stated security objectives. We assume a public key infrastructure with a *Certification Authority (CA)* that issues public/private key pairs and certificates to vehicles. A certificate contains the node's public key, attribute list (e.g., to distinguish between RSUs, public emergency vehicles and regular vehicles), the CA identifier, the certificate lifetime, and the CA signature.

Each received packet is first submitted to a sequence of plausibility checks using the packet's time and location fields as inputs. If at least one test fails, the packet is discarded.<sup>5</sup> Otherwise, if all checks succeed, the packet is validated cryptographically. First, the certificate is validated, unless it was previously validated and cached. Then, the signature(s) on the packet are validated and, if failed, discarded. Otherwise, the packet is processed further. We discuss in more detail the security mechanisms hereafter.

##### A. Cryptographic Protection

We use asymmetric cryptography and digital signatures for all messages. In the case of *beacons* (one-hop communication) a single signature is applied, with the source signing the whole PBR packet. This is straightforward since there are no intermediate nodes which change PBR header fields. In contrast, for multi-hop communication, additional protection is necessary for the mutable fields in the PBR headers.

An end-to-end signature by the packet's source can only cover the immutable fields. To enhance the protocol robustness, we proposed the combination of hop-by-hop (neighbor-to-neighbor) and end-to-end (source-to-destination) security: we propose a scheme protecting packets with two signatures: the *source signature*, calculated by the source over the immutable fields, and the *sender signature*, generated by each sending node over the mutable fields (Fig. 3).

On reception of a packet, a forwarding node *i*) verifies both the source and sender signature, *ii*) updates the mutable field values and generates a new sender signature, *iii*) replaces the old signature by the new one, and *iv*) re-forwards the packet. The destination node verifies both the sender and source signatures.

This approach pertains to packets that propagate across multiple hops, i.e., geo-unicast and geo-broadcast, as well as location service query and response.

##### B. Plausibility Checks

Hereafter is a selection of plausibility checks, which extend those presented in [10]. On reception of a packet, a node executes the different checks in sequence, and drops the packet if any of them fails.

<sup>5</sup>Even though signatures provide non-repudiation, we do not try to maintain state on nodes transmitting implausible information.

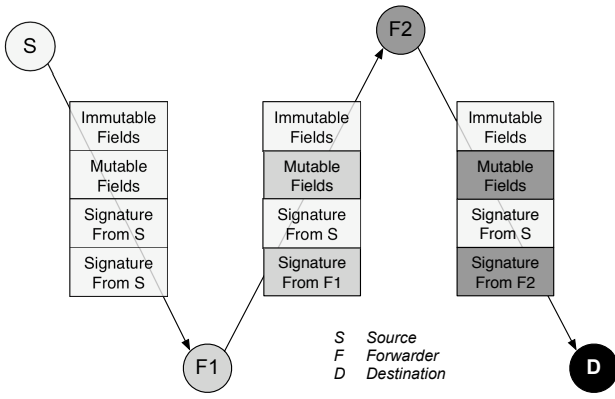


Fig. 3. Hybrid signature scheme: a packet holds a source and a sender signature

a) *Time*: A timestamp is checked for being in a time window to ensure that it is neither too old (in order to prevent replay attacks), nor it does not lie in the future. In fact, nodes update their location table only if the information of the PBR header is newer. This test ensures that an attacker cannot alter the destination position of a multi-hop packet and impose this information to all subsequent forwarders by setting the timestamp to a future value.

b) *Acceptance Range*: Assuming that communication devices have a maximum transmission range  $\Delta_{max}$ , no neighbor can be further away than  $\Delta_{max}$ .

c) *Velocity*: The maximum velocity of vehicles is limited by physical laws to  $v_{max}$ . Therefore, a claimed position update should be within a predicted space window, calculated around the node's previous position and a radius of  $\Delta_{time} * v_{max}$  ( $\Delta_{time}$  is the time between two consecutive position updates).

### C. Robustness Mechanisms

As the injection of false multi-hop floods or broad- or geo-casts wastes resources of a large network part, we propose rate-limiting mechanisms according to the attributes of the sending node. If the rate of such traffic originating from a node exceeds a protocol-specific threshold, its packets are not forwarded any further. Digital signatures and unique identification (source time-stamps) of the sender and the transmissions allow this throughout the network. To exert even tighter control, yet maintain effectiveness, we define distinct thresholds for different types of nodes. Furthermore, the description of the transmission (e.g., the target geographic area) can correspond to different thresholds. For example, private vehicles can be disallowed to initiate geo-casts beyond a given area size and allowed to do so at the lowest rate, while RSU units or emergency vehicles can do the same for larger areas and at higher rates.

## VI. ANALYSIS

### A. Achieved Security Level

Digital signatures and certificates prevent impersonation, modification and unauthorized (without the proper credentials) injection of packets. Thus, an external attacker (i.e., not a legitimate member of the network) can only replay control or

data packets. Recall that attacks such as jamming are beyond the scope of this paper.

Message freshness is achieved due to time-stamps, and duplicate detection at receivers. Spoofing attacks on the GPS signal, if this is used, are out of scope; we assume that nodes have their correct coordinates and reference time.<sup>6</sup>

A Sybil attack is prevented if private/signing keys are stored in a tamper-resistant unit performing all the cryptographic operations. It is thwarted, because attackers cannot share their private keys or obtain private keys of legitimate nodes. The *location service* is protected by the digital signature scheme: an attacker cannot impersonate a sought node nor alter the sought coordinates in the reply packet (assuming the destination is correct node).

The combination of plausibility checks at first prevents an attacker from relaying beacons or packets of other nodes: the coordinates and time-stamp in the beacon will prevent this. Either the coordinates of the replayed packet sender will be beyond the perceived nominal range (distance), or they will be correct but correspond to a sender that was in the given location at some point in the past.

The only option for the attacker is to declare a false own location, but its attack possibilities and impact are drastically reduced by plausibility checks. At most, the attacker can perturb its own position, perhaps adjust it with respect to the positions of its neighbors, but only within the limits of what is deemed plausible (according to plausible kinetic changes of the vehicles and the communication capabilities of the nodes).

An attacker cannot create a loop, as it cannot mount a Sybil attack. It might, under special conditions, cause a gap avoidance (see for example [1]) even if no gap is present. But this will only cause a mild lengthening of the end-to-end route. Of course, a loop can be formed and include *only* attackers, but this would be equivalent to the first attacker in the loop dropping the packet.

An attacker cannot misuse the plausibility checks against correct nodes: no reputation is maintained, and, for example, a replayed (implausible) beacon will *not* cause the blacklisting of an otherwise correct node. Furthermore, packet injection attacks have low impact on the network performance, as the vehicles entitled for higher-volume transmissions are more trustworthy.

### B. Comparisons With Alternative Signature Schemes

Hop-by-hop (HbH) signatures are not sufficient for protecting end-to-end multi-hop traffic, since end nodes can be impersonated. In contrast, end-to-end (E2E) signatures over the immutable fields relieve forwarders from cryptographic operations.<sup>7</sup> This E2E authentication does not protect the mutable field; an attacker could poison the location table its neighbors. Disabling such updates for the sake of security could impact the performance of the protocol (e.g., less responsive to mobility and connectivity changes).

<sup>6</sup>Future positioning systems will be secured, as is the case for the upcoming European system GALILEO.

<sup>7</sup>Authentication of the sender can be beneficial though.

An alternative apparently stronger than our hybrid scheme is an incremental signature scheme: the source signs the whole packet; each forwarder copies the received mutable fields to the end of the packet, updates its own mutable field, and appends a signature over the resultant packet. This way, the destination can authenticate every forwarder (and build a larger network view), and track the changes of the mutable fields. Yet, as the PBR operation is largely hop-by-hop (e.g., location of neighbors more important) and perturbation of own location is possible, the incremental scheme does not provide significant advantages of the hybrid one.

Tab. I presents the performed cryptographic operations (number of signature generations  $G$  and verifications  $V$ <sup>8</sup>) for a source, a forwarder, and the destination. Furthermore, the total overhead for communication over  $n$  forwarders is given. The hybrid scheme offers a desirable trade-off between achieved security and induced overhead.

	SOURCE	FORWARDER	DESTINATION	TOTAL
HbH	$G$	$G + V$	$V$	$G + V + n(2G + V)$
E2E	$G$	$V$	$V$	$G + (n+1)V$
Hybrid	$2G$	$2V + G$	$2V$	$G + (n+1)(2V + G)$
Incremental	$G$	$G + (n_{prev} + 1)V$	$G + (n+1)V$	$(n+2)G + \sum_{k=1}^{n+1} kV$

TABLE I  
NUMBER OF CRYPTOGRAPHIC OPERATIONS NEEDED

### C. Initial Measurement Results

To assess the deployability of our security solution, we have enhanced our existing prototype for car-to-car communication developed in the project *NoW – Network on Wheels*<sup>9</sup> with the proposed security mechanisms and performed measurements. The security implementation uses the OpenSSL library, ECDSA with a key size of 160bits for nodes and 224 bits for the CA. The measurements were conducted on a notebook with Intel Pentium M 1,6 GHZ CPU, 256 MB RAM, and Linux operating system. Each measurement was repeated 100 times. Signature generation for a beacon took  $\approx 2.9$  ms, processing of a signed beacon  $\approx 7.7$  ms. We regard this initial result as sufficient, but it should (and can<sup>10</sup>) be optimized, especially for beacons received at a high rate in a dense network scenario with many vehicles. We also measured in a lab setup the end-to-end delay of a packet sent over a 4 node multi-hop chain. For a packet with 100 bytes payload, the end-to-end delay was  $\approx 77.6$  ms, which satisfies the latency constraint (delay  $\leq 100$  ms) identified by [19] under idealistic conditions.

## VII. CONCLUSION AND FUTURE WORK

We have presented a solution to secure a position-based routing protocol for wireless multi-hop communication in vehicular ad hoc networks. Our solution combines digital

signatures/certificates, plausibility checks, and rate limitation. Digital signatures on a hop-by-hop and end-to-end basis provide authentication, integrity and non-repudiation. Plausibility checks reduce the impact of false positions on the routing operation. Rate limitation reduces the effect of packet injection on a large part of the network.

A main characteristic of the solution is its deployability due to usage of well-established security mechanisms. The integration in our experimental prototype for vehicular communication has shown a low implementation complexity. In a follow-up of this paper we will present a more detailed security analysis, additional plausibility checks, and protocol optimizations, as well as extensive experimental performance evaluation based on our testbed.

## REFERENCES

- [1] B.N. Karp and H.T. Kung. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. In *Proc. MobiCom*, Boston, MA, USA, 2000.
- [2] H. Füllner, M. Mauve, H. Hartenstein, M. Käsemann, and D. Vollmer. Location-Based Routing for Vehicular Ad-Hoc Networks. In *MobiCom*, 2002.
- [3] A. Festag, H. Füllner, H. Hartenstein, A. Sarma, and R. Schmitz. FleetNet: Bringing Car-to-Car Communication into the Real World. In *Proc. ITS World Congress*, 2004.
- [4] IEEE. Draft Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages. IEEE P1609.2/D3, 2005.
- [5] P. Papadimitratos, V. Gligor, and J.-P. Hubaux. Securing Vehicular Communications - Assumptions, Requirements and Principles. In *Proc. ESCAR*, 2006.
- [6] E. Fonseca and A. Festag. A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS. Technical Report NLE-PR-2006-19, NEC Network Laboratories, 2006. Available at <http://www.network-on-wheels.de>.
- [7] M. Raya and Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proc. SASN*, 2005.
- [8] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller. Attacks on Inter Vehicle Communication Systems - an Analysis. In *Proc. WIT*, 2006.
- [9] M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing Vehicular Communications. In *IEEE Wireless Communications Magazine*, 2006.
- [10] T. Leinmüller, C. Maihöfer, E. Schoch, and F. Kargl. Improved Security in Geographic Ad Hoc Routing Through Autonomous Position Verification. In *Proc. VANET*, 2006.
- [11] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer. Influence of Falsified Position Data on Geographic Ad Hoc Routing. In *Proc. ESAS*, 2005.
- [12] T. Leinmüller and E. Schoch. Greedy Routing in Highway Scenarios: The Impact of Position Faking Nodes. In *Proc. WIT*, 2006.
- [13] J.-H. Song, V.W.S. Wong, and V. C.M. Leung. A Framework of Secure Location Service for Position-based Ad hoc Routing. In *Proc. PE-WASUN04*, 2004.
- [14] H. Takagi and L. Kleinrock. Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals. *IEEE Transactions on Communications*, 4(32):246–257, 1984.
- [15] E. Schoch, E. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos. Impact of Pseudonym Changes on Geographic Routing in VANETS. In *Proc. ESAS*, 2006.
- [16] E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar. Support of Anonymity in VANETS Putting Pseudonymity into Practice. In *Proc. WCNC*, 2007.
- [17] B. Schneier. Attack Trees: Modeling Security Threats, 1999.
- [18] Charles Harsch. Secure Position-Based Routing. Master's thesis, Swiss Federal Institute of Technology, Lausanne (EPFL), 2007.
- [19] US Vehicle Safety Communications (VSC) Consortium. <http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm>.

<sup>8</sup>The verification operation comprises verification of the received certificate and verification of the signature.

<sup>9</sup><http://www.network-on-wheels.de>

<sup>10</sup>Optimizing the cryptographic library, using cryptographic hardware, smaller key sizes according to their certificate lifetime, caching received certificates, etc.