Greedy Routing in Highway Scenarios: The Impact of Position Faking Nodes

Tim Leinmüller[+] and Elmar Schoch[*]
[+]DaimlerChrysler AG, Research Vehicle IT and Services, Tim.Leinmueller@DaimlerChrysler.com
[*]University of Ulm, Department of Media Informatics, Elmar.Schoch@uni-ulm.de

***Abstract*— Vehicular Ad-Hoc networks (VANETs) have been an active research domain during the past few years. Work so far focused on routing and applications, however, research on security issues has been started only recently. One of the fundamental results of past and ongoing research projects in the domain of vehicular ad-hoc networks is the usage of geographic routing protocols. On the one hand this is due to the fact that they are well suited to highly dynamic network topologies. On the other hand VANETs are assumed to provide location based services, which would also benefit from position aware routing.**

In this paper, we analyze the potential impact of false position information in beacon messages on geographic routing. We assume that false position information is distributed either by malicious nodes or by defective nodes. For the analysis, we focus on highway scenarios with respective vehicular movement patterns. Our results show severe performance degradation even in case there is only a low percentage (10%) of maliciously acting nodes that combine position information falsification with subsequent message dropping.

***Index Terms*—Vehicular ad hoc networks (VANETs), position dependent routing, security**

I. Introduction

The common goal of projects on vehicular ad hoc networks (VANETs) is the intention to improve vehicle passengers' safety by means of inter-vehicle communication. So, for instance in the case of an accident car to car communication might be used to warn approaching cars. Research projects such as Fleetnet [1] or CarTALK [2] have already produced fundamental results in the domains of routing and applications. In Fleetnet, geographic routing has been selected as routing scheme due to its compliance with application needs and its good performance under extremely dynamic network conditions [3]. Ongoing work is concentrating on further evaluation of these results as well as on the definition of common standards amongst car manufacturers (like in the C2C-CC [4] or the VSCC [5]). Another important direction is the research on security and privacy issues of VANETs. In this paper we address the security of geographic routing in highway scenarios in terms of analyzing the impact of position information on routing performance.

Geographic routing approaches mostly share common principles. Every node knows its current position, e.g. by using a positioning system such as GPS. This position is periodically broadcasted in beacon messages so that nodes within the wireless transmission range are able to build up tables of neighboring nodes including their position. If a node has to forward a packet it selects one of the neighboring nodes as next hop, according to a predefined rule, e.g. the node closest to the destination.

Obviously, when a node disseminates wrong positions, the routing process is influenced. Wrong position information may result from malfunction in the positioning hardware or it may be falsified intentionally by attackers to reroute data. In [6] we have analyzed possible attacks and effects on routing that arise from wrong position claims. Simulations have shown that malfunctioning nodes may degrade the performance of a system to some extent, whereas rerouting data through malicious nodes violates basic security goals such as confidentiality, authenticity, integrity, or accountability. While our previous work primarily investigated the effects in complex city scenarios, we now detail the analysis of security-relevant effects of falsified position information regarding scenarios with vehicles on long-range highways. We will point out that movement patterns of vehicles in long-range highway scenarios result in additional security hazards.

The next section will give an overview on related work regarding position dependent routing and position information in VANETs. Then, section III points

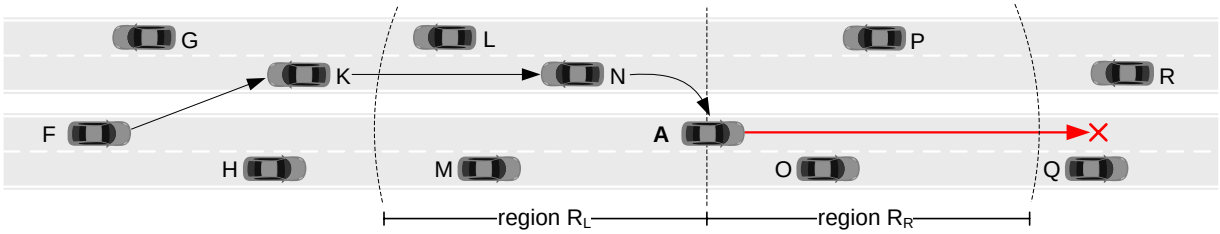

Fig. 1
GREEDY ROUTING ON A HIGHWAY, MOBILE ATTACKER

out the particular problems of position information in highway scenarios and thus the motivation for a closer look into these scenarios, followed by section IV, which depicts and analyzes simulation results of the effects of malicious behavior. Finally, section V concludes the paper.

II. RELATED WORK

Geographic routing for vehicular ad hoc networks has been investigated intensely. In [3] Mauve et al. provide an overview and a classification of packet forwarding schemes based on individual node position.

In VANETs, most commonly the class of greedy routing approaches is used. All greedy approaches have in common that the next hop node of a packet has to be closer to the destination's position than the current node. In case multiple neighbors satisfy this criterion, several selection strategies have been proposed. The greedy-only method selects the neighbor with the smallest Euclidean distance to the destination. In contrast, Most Forward progress within Radius (MFR) [7] projects the positions of suitable neighbors onto a straight line stretched across the current node's position and the destination's position. Then, the neighbor with the most "progress" on that line is chosen. Other greedy methods select the next hop randomly or by the minimal distance to the current node (Nearest with Forward Progress, NFP [8]) in order to save sending power. Obviously, all greedy methods are stuck if there is no neighbor closer to the destination's position. The perimeter routing in GPSR [9], [10] is one proposal as recovery strategy in such situations, caching the packet until a suitable neighbor appears is another [11].

Regarding the influence of position information on routing Kim et al. have conducted examinations on the impact of location inaccuracies in [12]. They defined a scheme to classify localization errors and used it in simulations with relative location errors ranging from $0m$ up to $50m$. Their results show some effects like routing loops that have also been observed during our work, under the assumption of malicious nodes.

Apart from these observations of localization errors and our previous work in [6], there has been no work on security concerns specific to effects of falsified position data in geographic ad hoc routing.

III. MOTIVATION AND SCENARIO ANALYSIS

The in-detail look on highway scenarios is motivated by several aspects. First, highways represent a considerable part of road network which renders them an important application area for inter-vehicle communication powered active safety systems. Second, many applications currently investigated are specific for usage on highways.

Furthermore, mobility characteristics on highways follow simple schemes and are predictable to a certain extent, i.e. no vehicles leave the highway between two ramps, therefore only two directions for node movements exist for many kilometers. In addition, nowadays high usage of highways and thus the significance of highways in general may also attract additional attention of potential malicious nodes, regardless whether they are part of the network in a vehicle or act from the roadside. These circumstances turn VANETs on highways into a likely target for attackers.

Figure 1 depicts an example scenario, in which an attacker A attempts to control communication in the VANET along a highway. In this example, we assume the attacker to be mobile, e.g. to be a normal car moving with other vehicles on the highway. Beaconing as the base of geographic forwarding requires nodes to broadcast their position periodically. To reach his goal, the attacker A may announce a position displaced in one direction of the road. In case he chooses

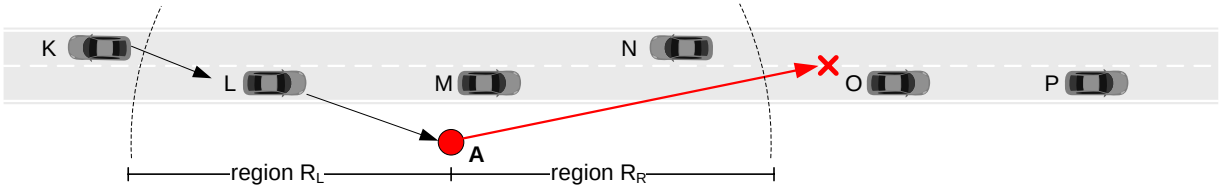

Fig. 2
GREEDY ROUTING ON A HIGHWAY, STATIONARY ATTACKER

a suitable distance between real and forged position, he appears to be the optimal forwarding node for other vehicles assuming faultless operation, at least for all packets being passed on in the direction the attacker displaced his position in. Thus, in figure 1 for instance a packet from F to Q is routed over the attacker A, who pretends to be at the position denoted by X, whereas the packet normally should have been routed via O, if A had announced its correct position.

The second scenario as displayed in figure 2 is quite similar, yet it differs in an important detail. Here we assume the attacker A to be stationary at the road-side (road-side attacker), e.g. in the most simplistic case a person with a laptop. So, in this case the attacker targets a fixed area with highly varying neighbors, whereas in the previous example the attacker targets his neighborhood, which in contrast remains quite stable, according to vehicle movement patterns on highways.

Independent of the attacker A being mobile or immobile, assuming a given wireless transmission range, it can be proven that A is theoretically able to grab all packets along the highway in one direction only by claiming its own position farther down the highway than the maximum communication distance. In this case, no ordinary node in region R_R is able to supersede A's position when nodes in region R_L forward packets from left to right.

Grabbing of packets in one direction may be even extended to both directions, in case an attacker manages to impersonate two node identities in parallel that are used routing. This is also called "Sybil attack". So, using the same proceeding with a second identity in exactly the mirrored way, A is additionally able to intercept packets in the second direction. Then, A is theoretically able to intercept all data traffic passing along the highway.

In summary, VANET communication along highways is highly vulnerable to attacks based on forged position information and thereby a likely target for maliciously acting nodes. Following this motivation and the scenario analysis in this section, in the next section we will evaluate simulation results with mobile and stationary attackers.

IV. SIMULATION RESULTS

In order to estimate effects of falsified position information on geographic greedy routing, we conducted simulations with the simulator ns-2 [13]. To be comparable with previous results, the simulation setup is similar to the one in [6], apart from the vehicle movement patterns. The simulation parameters are summarize in table I. In short, simulated nodes are equipped with an IEEE 802.11 wireless transceiver sending at $1Mbps$ with a radio range of $250m$. Packet routing applies a greedy scheme that selects as next hop the neighbor closest to the geographic packet destination. Moreover, routing mechanisms cache packets temporarily that cannot be forwarded instantly.

In this work, we use realistic traffic patterns on $13km$ of a highway with two lanes per direction and about six vehicles per kilometer and lane. The movement patterns were produced by the DaimlerChrysler driver behavior simulator called FARSI.

While the overall simulation endures 60 seconds, 100 messages are sent during the first 30 seconds. Source and destination of messages are set in two separate ways. One of these patterns sets them completely random imitating the diversity of messages flowing around. The other pattern divides the highway into two parts with equal length and assures that source and destination are located in different partitions.

In parallel to different data traffic scenarios, we model two separate variants of attackers. On the one hand, a certain percentage of nodes falsifies its position and optionally drops messages. On the other hand, a single attacker is positioned stationary in the

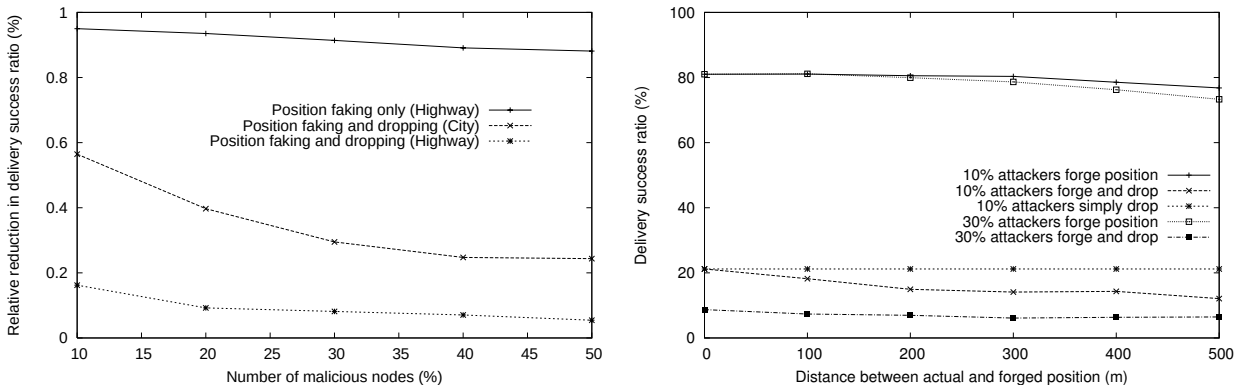

Fig. 3

A) RELATIVE REDUCTION IN SUCCESSFULLY DELIVERED MESSAGES DEPENDING ON MALICIOUS NODE PENETRATION
B) ABSOLUTE DELIVERY SUCCESS RATIO DEPENDING ON DISTANCE BETWEEN REAL AND FORGED POSITION

Parameter	Value
Length of highway (km)	13
Node density (nodes/km/lane)	~ 6
Max. node velocity (m/s)	~ 50
Pause times (s)	0.0
Mobility model	FARSI scenarios
Link-/MAC-Layer	IEEE 802.11
Transmission range (m)	250
Number of sent messages	100
Simulation time (s)	60
Simulation runs	20

TABLE I
SHORT OVERVIEW ON SIMULATION PARAMETERS

middle of the scene resembling an attacker sitting besides the highway (road-side attacker). In combination with messages' source and destination in opposite parts of the highway, we thereby make sure that the messages pass the attacker. Jointly, this pattern of traffic and this kind of attacker clearly demonstrates the severe impact of position falsification.

Figure 3a shows the relative reduction in successfully delivered messages when applying position faking in highway scenarios, once with and once without subsequent dropping of packets at malicious nodes. Attackers as well as packet sources and destinations are distributed randomly over the highway scene. In addition, a city scenario with position faking and packet dropping is also included for comparison.

The ratio of successfully delivered packets decreases about 5% if 10% of all nodes forge their position and does not get dramatically worse even with 50% of forging nodes. This is depicted for the highway scene but also holds for the random waypoint model used as city scenario (not depicted here).

Compared to these results, delivery success ratio breaks down when attackers also drop packets. In city scenarios, we observe a decrease from 40% to 80%, whereas the performance in highway scenes decreases by approximately 85% already with only 10% of malicious nodes. It is also important to notice that the delivery ratio decreases only little in dependence of the number of position faking nodes, which results from the linear node distribution on highways and the resulting routing paths.

Whereas in city scenarios, packet delivery most likely can be accomplished via several geographically distinct routing paths and the decision for one of these paths is influenced by minor movements of intermediate nodes, in highway scenarios routing paths are restricted to the quasi-linear geographic region of the highway. Thus if an attacker succeeds in pretending to be the optimal next hop for nearly all packets relayed by its neighbors, what is achievable by falsifying position informations in beacons, the attacker has far more influence on the overall network performance than in geographically more distributed scenarios, i.e. city scenarios.

Figure 3b shows the effect from an other point of view. While falsifying the own position with growing degree has only marginal influence on delivery ratio, combined falsifying and dropping shows more degradation though on a completely different level.

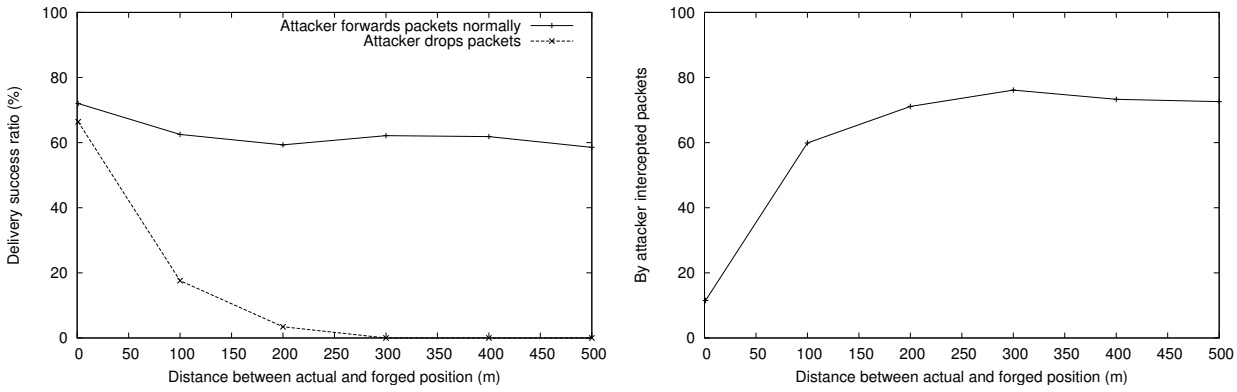

Fig. 4

A) SUCCESSFULLY DELIVERED MESSAGES AND B) INTERCEPTED PACKETS WITH SINGLE STATIONARY ATTACKER

When 10% of all nodes simply drop packets without forging positions, the absolute delivery success ratio decreases to 20% in our scenario. This number decreases further if attackers also forge their position. Besides, the curves also do not break down to zero which is mainly due to random traffic. Therefore, some packets with short distance between source and destination never pass a malicious node.

To be able to quantify the effectiveness of simple falsifying, we simulated the more specific scenario of the stationary attacker. The method of attacking, i.e. forging the own position claim, packet dropping and other parameters are adopted from previous simulations. Unlike before, we assume a single attacker but assure that all sent packets have to pass the attacker by choosing source and destination appropriately. Thus we are able to estimate the number of intercepted packets directly. In other words, we now take a microscopic point of view, whereas results above represent a more macroscopic approach.

The results of these simulations are given in figure 4. First, if we look at the overall number of packet delivery successes in figure 4a, we see again, that forging the own position claim does not cause major influences. In fact, almost all packets are routed through the single attacker besides the highway. This gets clear when the attacker refrains from forwarding packets and simply drops them. In that case the ratio of successfully delivered messages reduces to zero when the attacker falsifies its position to $300m$ further down the road.

We get the same picture when we look at the number of intercepted packets by the attacker. In figure 4b, almost 80 of 100 packets are intercepted – the remaining packets do not reach their destination due to routing itself.

V. CONCLUSIONS

Communication in vehicular ad hoc networks on highways is highly affected by nodes distributing falsified position information. In this paper we have shown that malicious nodes are able to divert and drop regular traffic, which results in serious network performance degradation. Our simulation results show that in highway scenarios the impact is even more severe than in city scenarios [6]. 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 in city scenarios, 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.

In current research, we develop and evaluate methods to detect maliciously acting nodes, in order to lower the effects of faked position information. These methods comprise detection techniques and countermeasures, which are divided into single node and cooperative functions.

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," `http://www.cartalk2000.net`, 2004.

[3] Martin Mauve, Jörg Widmer, and Hannes Hartenstein, "A survey on position-based routing in mobile ad-hoc networks," *IEEE Network*, vol. 1, no. 6, pp. 30–39, Dec. 2001.

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

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

[6] 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.

[7] Hideaki Takagi and Leonard Kleinrock, "Optimal transmission ranges for randomly distributed packet radio terminals," *IEEE Transactions on Communications*, vol. 32, no. 3, pp. 246–257, Mar. 1984.

[8] Ting-Chao Hou and Victor Li, "Transmission range control in multihop packet radio networks," *IEEE Transactions on Communications*, vol. 34, no. 1, pp. 38–44, Jan. 1986.

[9] S. Giordano, I. Stojmenovic, and L. Blazevie, "Position based routing algorithms for ad hoc networks: a taxonomy," *IEEE Communications Magazine*, vol. 40, no. 7, pp. 128–134, July 2001.

[10] B. Karp and H.T. Kung, "Greedy perimeter stateless routing for wireless networks," in *Proceedings of the Sixth ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000)*, Boston, USA, Aug. 2000, pp. 243–254.

[11] 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.

[12] Yongjin Kim, Jae-Joon Lee, and Ahmed Helmy, "Impact of location inconsistencies on geographic routing in wireless networks," in *Proceedings of the 6th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems (MSWIM '03)*. 2003, pp. 124–127, ACM Press.

[13] "Network simulator ns-2," http://www.isi.edu/nsnam/ns/, 2004.