Influence of Falsified Position Data on Geographic Ad-Hoc Routing

Tim Leinmüller[+], Elmar Schoch[+], Frank Kargl[*] and Christian Maihöfer[+]

[+]DaimlerChrysler AG, Research Vehicle IT and Services
{Tim.Leinmueller|Elmar.Schoch|Christian.Maihoefer}@DaimlerChrysler.com
[*]University of Ulm, Department of Media Informatics
Frank.Kargl@informatik.uni-ulm.de

Abstract. There has been a lot of effort in the research on routing in mobile ad hoc networks in the last years. Promising applications of MANETs, e.g. in the automotive domain, are the drive for the design of inter-vehicle networks. So far, several projects in this field have chosen geographic routing approaches because of their outstanding performance and the possibility to support location-based applications like traffic warning functions. Having reached a reasonable functional level, a next step will be a deeper study of safety and security issues.
With this paper, we dive into that area by assuming defective or malicious nodes that disseminate wrong position data. First, we have a look at the local problems that may arise from falsified position data, then we show the global effects on the routing performance by simulating malicious nodes. Simulation results show that the overall ratio of successfully delivered messages decreases, depending on the number of maliciously acting nodes, even up to approximately 30%. We conclude from this result that future work should take these threats into account in order to design more robust routing protocols.

1 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 [1]. Main target of these projects is the improvement of vehicle safety by means of inter-vehicle communication. So e.g. in the case of an accident, a VANET might 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.

[1] e.g. projects like Fleetnet [1] or CarTalk2000 [2]

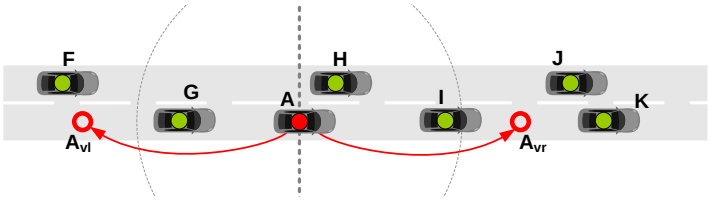

Fig. 1. Vehicle A pretends to be at positions A_{vl} and A_{vr} and thus manages to grab all traffic along the road.

Now European and US car manufacturers are taking the next step in projects that aim at defining a reference architecture and suitable standards for VANETs[2].

In contrast to generic MANETs, where mostly topology-based routing protocols are being developed, many of the VANET projects use position-based routing mechanisms [6] for establishing connectivity between vehicles. This offers some advantages in performance and the possibility to address vehicles by their position (so called Geocast) instead of their address.

Whereas a lot of effort was already put in securing traditional MANETs [7,8], the security research for position-based routing and VANETs is still in its infancy. [9] 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.

When false position information is distributed in the VANET, this can severely impact the performance of the network, as we will show in this paper. 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, e.g. by cryptographic means, this can lead to a compromise of nearly all security goals like confidentiality, authenticity, integrity, or accountability.

Figure 1 shows a scenario where node A claims to be at two additional (faked) positions A_{vl} and A_{vr}. Based on a greedy forwarding strategy, nodes always select the node nearest to the destination as the next forwarding node. Assuming that F wants to send a packet to node K, it will first sent the packet to its only direct neighbor G. G will then forward the packet to the node nearest to the destination from which it can hear beacons. This seems to be A_{vr}, so

[2] e.g. the US Vehicle Safety Communication Consortium (VSCC) [3], the Network on Wheels project (NoW) [4], or the Global Systems For Telematics (GST) [5] initiative

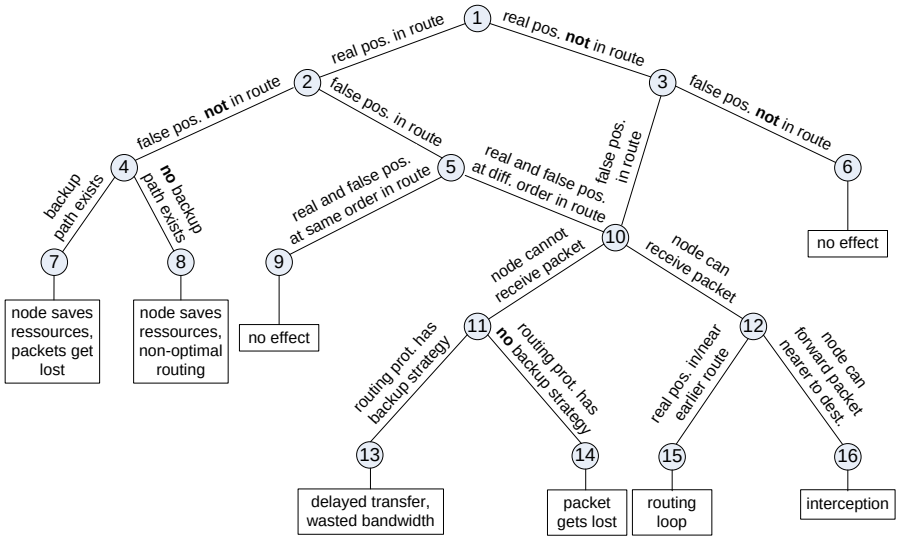

Fig. 2. Possible effects of false position data

the packet ends up at node A, which can now forward, modify or discard it at will. In the opposite direction, the packet from K will go to I, which will again send it to the assumed best node A_{vl}. So faking only two positions, A is able to intercept all traffic along the road.

The remainder of this paper is organized as follows. The next section will give a more complete discussion on the effects of false position data. Section 3 provides our simulation results. In section 4 we discuss related work and section 5 concludes our work.

2 Effects of False Position Data

If we assume that false position data is generated by malfunctioning or malicious nodes, what are the possible effects?

Figure 2 shows some of the effects that can occur. If a node's real position is not in the route from source to destination and neither is the false position, then no effect occurs (6). The same is true if real and false position are in the route, but the positions are similar and the position within the route does not change (9).

A node that does not want to be used for forwarding, e.g. to save own resources like energy, bandwidth, etc, may choose to fake a position outside the route (4). Depending on whether there is a backup path (7) or not (8), either packets get lost or at least the routing becomes non-optimal.

Finally, the cases below position (10) can either be reached, if real and false position are both in the route but at different positions, or if the real position

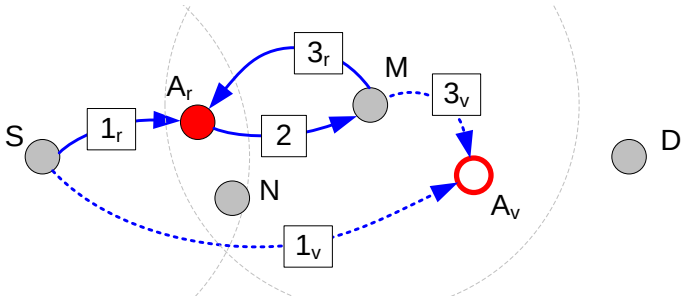

Fig. 3. Routing loop induced by the malicious node A which pretends to be at A_v rather than at its actual position A_r

is not in the route but the false is. Then one has to distinguish, if the node can receive the packet sent to the false position at his real position (12) or not (11).

In case (11), the packet sent to the node is lost. If the routing protocol notices that (e.g. by means of acknowledgments or timeouts) and has a backup strategy (13), the packet may still be delivered to the destination. This will create an additional delay and waste bandwidth, as the first transmission gets lost. If the routing protocol has no such backup strategy, the packets get lost (14).

In case (12), the node receives the packet. If the real position of a node allows the packet to be delivered to a position which is nearer to the destination than the false position (16), then the packet will reach its destination. The benefit of an attacker might be, that he can intercept traffic that would otherwise be routed around him, sniffing e.g. confidential information or similar.

If the real position of the node is further away from the destination than the false position (15) and the node will then forward the packet so it reaches the false position again, routing loops can occur as shown in figure 3. Here node A claims to be at position A_v where its real position is A_r. S sends the packet to the node in its neighborship that claims to be nearest to D (1_v). In reality, node A receives the packet (1_r). It then forwards the packet to node M (2) which again tries to forward it to the node that is nearest to D (3_v). This is the virtual position A_v and so the packet is again received by A (3_r). The steps 2 and 3_r repeat forever or until a time-to-live counter expires.

As we have shown, false position data is clearly an issue that can affect the performance, reliability and security of a MANET using position-based routing. In the next section we will use simulations to show, how severe this impact can be for certain scenarios.

3 Simulative Analysis

3.1 Simulation Environment

In order to be able to estimate the impact of falsified position data on geographic routing, we have implemented position faking in the ns-2 simulation

Parameter	Value
Number of nodes	100
Length of square node field	1000 – 4000m
⇒ node density (nodes/km^2)	6,25 – 100
Max. node velocity (m/s)	50
Pause times (s)	0.0
Mobility model	Random Waypoint
Link-/MAC-Layer	IEEE 802.11
Transmission range (m)	250
Number of sent messages	100
Simulation time (s)	40
Simulation runs	20

Table 1. Short overview on simulation parameters

environment. For the routing scheme, we choose a greedy based approach. It selects the neighbor node as next hop for a packet, whose distance to the destination is minimal. Like all greedy methods, this algorithm fails if no neighbor is found that is closer to the destination than the current node itself. The deployed recovery strategy is based on a caching approach, i.e. packets are stored locally until either a suitable neighbor is reachable or until the node decides to drop the packet (see [10]).

Besides ordinary routing, we also have to integrate a model of maliciously acting nodes. Therefore, a certain percentage of all nodes in the simulation scenario behaves as follows:

1. 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 real position).
2. 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.

As data traffic, 100 messages are transmitted from a random source to a random destination. The messages are randomly created during the first 30 seconds of the simulation run. Further simulation parameters are listed in table 1. Node density, velocities and mobility model approximately reflect the movement patterns of vehicular traffic in an urban area [11].

The following subsections present and discuss our simulation results regarding the impact on ad hoc network routing performance. We take a look at the impact on the delivery ratio and the reasons for the impact, namely parameters such as number of packet drops due to routing loops and number of packets remaining in the routing caches.

3.2 Impact on Delivery Ratio

The influence of falsified position information on the overall number of successfully delivered messages has been measured in several simulation runs with different percentages of position faking nodes. Figures 4 and 5 contain the results of simulation runs in a $2000m * 2000m$ sized network field with 10% and 40% faking nodes, once with and once without packet dropping. In figure 4, the percentage of successfully delivered messages in total is depicted, whereas figure 5 shows the relative decrease compared to the case without falsified position information.

As expected, with position faking, the delivery ratio is always negatively influenced. In case faking nodes do also drop received packets, the impact is even more severe (see figure 4). The relative comparison in figure 5 shows, after an initial phase, pure position faking decreases the overall delivery ratio by approximately 4% for 10% faking nodes, or 12% for 40% position falsifying nodes. Position faking with dropping results in higher loss, namely about 20% respectively 32%.

Figure 6 contains the relative delivery ratio reduction for different network sizes, compared to the case without falsified position information. When malicious nodes do not drop packets, increasing network sizes continue to reduce the relative delivery ratio. With packet drops, we observe a maximum reduction at network sizes of $2500m * 2500m$. This is the result of two overlapping effects. On the one hand, with increased network size, the number of hops and thus the probability of encountering a malicious node increases. On the other hand, with sparse network density, the probability of unsuccessful delivery due to network partitioning increases anyway and leverages the effects of dropping. The latter effect is visualized in figure 7, where the overall delivery ratio is shown for different network area sizes.

3.3 Analysis of Reasons for Decreased Delivery Ratio

The decreased amount of successfully delivered messages in scenarios with position falsifying nodes has its origin in three different reasons of messages getting "lost" during their traversal of the ad hoc network. These three are, packet drops due to detection of routing loops, undelivered messages remaining in caches since no suitable next hop has been found and packets dropped by maliciously acting nodes. Obviously, the latter reason is only of importance in scenarios, where position faking nodes actually drop packets.

According to our assumptions made in section 2, one reason for the decreased ratio of successfully delivered messages is the higher amount of packet drops due to routing loops. Figure 8 shows the corresponding simulation results. As a general remark, larger network sizes result in higher number of intermediate hops and therefore in a higher probability for creation of routing loops. From the simulation results in figure 8, we see, packet drops resulting from detected routing loops do also occur, even if there is no falsified position information. This results from the combination of node mobility and packet caching as recovery strategy.

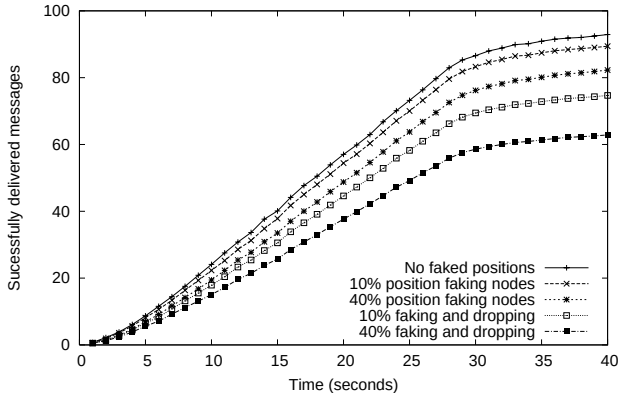

Fig. 4. Successfully delivered messages accumulated over simulation time

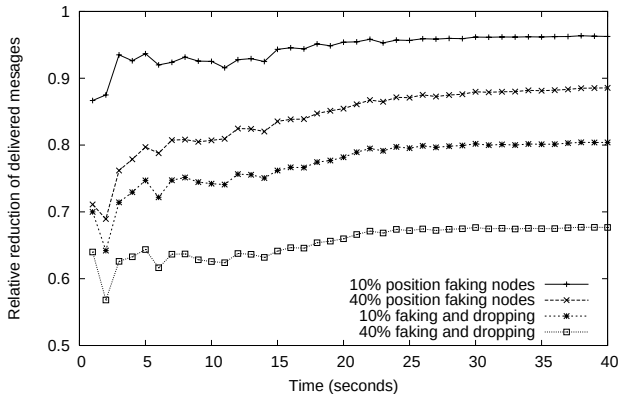

Fig. 5. Relative reduction of successfully delivered messages over simulation time

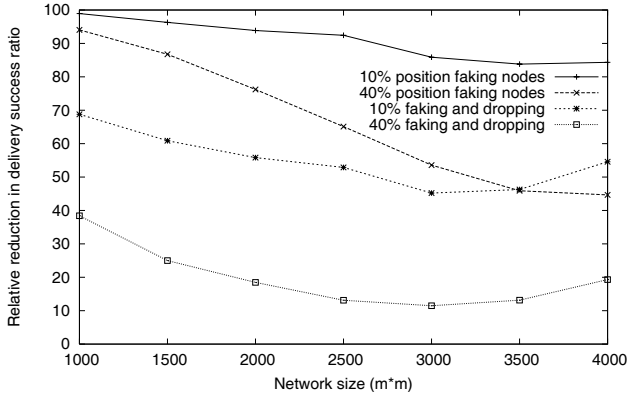

Fig. 6. Relative reduction of successfully delivered messages in dependence of network size

In scenarios, where position falsifying nodes do not drop received packets, the amount of packets dropped due to routing loops is always higher. On the other hand, it is obvious that if position faking nodes do drop received packets, i.e. before they can get into routing loops, this value has to be inferior.

The simulation results for the second reason for decreased delivery ratio, the amount of packets remaining in the node's caches, is shown in figure 9. According to these simulation results, in most cases falsified position information does not cause an increased number of packets remaining in the caches. For scenarios without packet dropping by maliciously acting nodes, the results are quite close to those of simulations without false position information. The increasing difference for larger network areas is caused by the increasing amount of packet drops in routing loops. And again, in case, maliciously acting nodes do drop packets, this effect can be neglected.

As an overall conclusion of this analysis, we retain the following. Depending on the behavior of position faking nodes, the following effects are responsible for the decreased ratio of successfully delivered messages. If the falsifying nodes do not drop packets, the main reason are packet drops resulting from detected routing loops. Their number is higher than the reduction of packets remaining in the routing caches compared to the case without faked positions. If the falsifying nodes maliciously do drop packets, the dropping itself is the dominant effect. Improvements regarding both other effects are only the result of less packets remaining in the network after those drops.

4 Related Work

The possibility of using *geographic* routing for mobile ad hoc networks has been investigated intensely. Especially the vision of ad hoc routing in vehicular networks was a stimulus for geographic routing research. This is due to the particular characteristics of such networks on the one hand and the necessity of geographic data distribution for the envisioned applications on the other hand.

Among the proposed packet forwarding schemes based on the individual node position, some main categories can be identified [6]. One of these comprises the *greedy routing* approaches. 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 were proposed. The greedy-only method selects the neighbor with the smallest Euclidean distance to the destination. In contrast, MFR (most forward progress within radius [12]) projects the positions of the 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 (NFP [13]) in order to save sending power. Obviously, all greedy methods are stuck if there is no neighbor closer to the destination's position. If packets shall not be lost at such a point, a recovery strategy must be introduced. The perimeter routing in GPSR [14] is one possibility, caching the packet until a suitable neighbor appears is another [10].

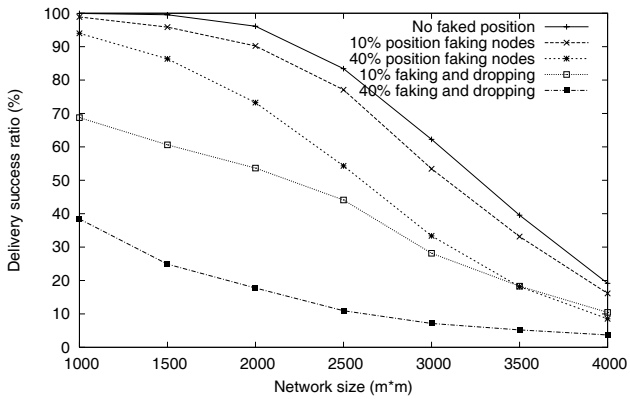

Fig. 7. Percentage of successfully delivered messages for different network sizes

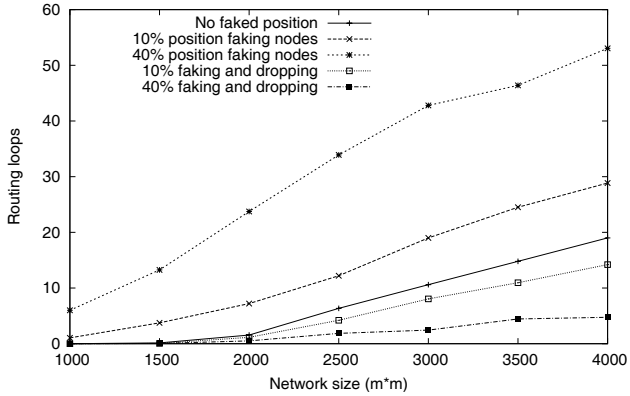

Fig. 8. Number of drops due to routing loops

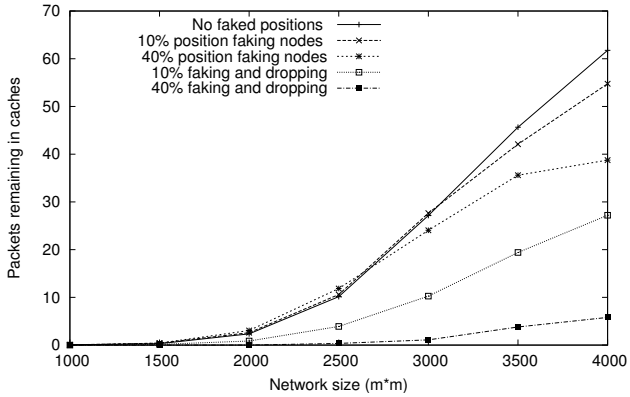

Fig. 9. Number of undelivered messages remaining in caches

A completely different geographic routing category uses *restricted directional flooding* [6]. For example, the LAR (Location aided routing) protocol by Ko and Vaidya [15] defines a rectangular region with the sender's position as one edge, and the destination's position as the diagonal opposed edge. Within that region, the packet is flooded. DREAM [16] acts very similarly, but uses a conus-shaped flooding region.

A third category of geographic routing applies hierarchical mechanisms. Terminodes [17], for instance, introduces two levels of routing. In a small region of several hops, a proactive routing is used, whereas larger distances are traversed by a special greedy method.

For vehicular ad hoc networks, geographic routing is particularly appropriate. 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 [18]. One reason is that topology-based protocols like DSR or AODV 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.

Kim, Lee and Helmy have conducted examinations on the impact of location inaccuracies on geographic routing [19]. They defined a scheme to classify localization errors and ran simulations with relative location errors ranging from $0m$ to $50m$. They simulated using GPSR, with and without perimeter mode. 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 in contrast to routing functionality, there has been no work on security concerns specific to effects of falsified position data in geographic ad hoc routing.

5 Conclusion

Falsified position information in mobile ad hoc networks with geographic routing protocols results in serious network performance degradation. In this paper we have presented an analysis of local and global effects of falsified position information. Our simulation results show that the overall delivery ratio might decrease even up to approximately 30%, depending on the number of maliciously acting nodes and depending on whether the malicious nodes drop packets or not.

Furthermore, we analyzed the reasons for decreased delivery ratio, which again, depend on the forwarding behavior of malicious nodes. Whereas for scenarios without packet dropping by position faking nodes, drops resulting from routing loops are the main reason, in scenarios with packet dropping by position faking nodes, the dropping itself is the actual reason.

In current research, we develop 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 co-operative functions.

References

1. Franz, W., Wagner, C., Maihöfer, C., Hartenstein, H.: Fleetnet: Platform for inter-vehicle communications. In: Proc. 1st International Workshop on Intelligent Transportatin (WIT'04), Hamburg, Germany (2004)
2. CarTalk 2000. (`http://www.cartalk2000.net`)
3. US Vehicle Safety Communication Consortium. (`http://http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm`)
4. Network on Wheels. (`http://www.informatik.uni-mannheim.de/pi4/lib/projects/NoW/links.html`)
5. Global Systems For Telematics. (`http://www.gstproject.org/`)
6. Mauve, M., Widmer, J., Hartenstein, H.: A survey on position-based routing in mobile ad-hoc networks (2001)
7. Kargl, F., Schlott, S., Weber, M., Klenk, A., Geiss, A.: Securing ad hoc routing protocols. In: Proceedings of 30th Euromicro Conference, Rennes, France (2004)
8. Kargl, F., Gei, A., Schlott, S., Weber, M.: Secure dynamic source routing. In: Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS-38), Hilton Waikoloa Village, HA (2005)
9. Hubaux, J.P., Čapkun, S., Luo, J.: The security and privacy of smart vehicles. IEEE Security and Privacy **4** (2004) 49–55
10. Maihöfer, C., Eberhardt, R., Schoch, E.: CGGC: Cached Greedy Geocast. In: Proc. 2nd Intl. Conference Wired/Wireless Internet Communications (WWIC 2004). Volume 2957 of Lecture Notes in Computer Science., Frankfurt (Oder), Germany, Springer Verlag (2004)
11. Saha, A.K., Johnson, D.B.: Modeling mobility for vehicular ad-hoc networks. In: VANET '04: Proceedings of the first ACM workshop on Vehicular ad hoc networks, ACM Press (2004) 91–92
12. Takagi, H., Kleinrock, L.: Optimal transmission ranges for randomly distributed packet radio terminals. IEEE Transactions on Communications **32** (1984) 246–257
13. Hou, T.C., Li, V.: Transmission range control in multihop packet radio networks. IEEE Transactions on Communications **34** (1986) 38–44
14. Karp, B., Kung, H.: 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 (2000) 243–254
15. Ko, Y., Vaidya, N.: Location-aided routing (lar) in mobile ad hoc networks. In: Proceedings of the Fourth ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 1998). (1998) 66–75
16. Basagni, S., Chlamtac, I., Syrotiuk, V.R., Woodward, B.A.: A distance routing effect algorithm for mobility (DREAM). In: Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Dallas, USA, ACM Press (1998) 76–84
17. Blazevic, L., Giordano, S., Boudec, J.L.: Self organized terminode routing. Technical Report DSC/2000/040, Swiss Federal Institute of Technology (2000)
18. Füssler, H., Mauve, M., Hartenstein, H., Käsemann, M., Vollmer, D.: A comparison of routing strategies for vehicular ad hoc networks. Technical Report TR-3-2002, Department of Computer Science, University of Mannheim (2002)
19. Kim, Y., Lee, J.J., Helmy, A.: Impact of location inconsistencies on geographic routing in wireless networks. In: MSWIM '03: Proceedings of the 6th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems, ACM Press (2003) 124–127