Vulnerabilities of Geocast Message Distribution

Elmar Schoch*, Frank Kargl*, Tim Leinmüller+ and Michael Weber*
* Ulm University, Institute of Media Informatics
{elmar.schoch|frank.kargl|michael.weber}@uni-ulm.de
+ DENSO AUTOMOTIVE Deutschland GmbH, Technical Research Department
t.leinmueller@denso-auto.de

***Abstract*—Geocast refers to the distribution of messages within a geographic destination region. This makes it an important paradigm for the application to vehicular ad hoc networks (VANETs), because most safety-related information needs to be delivered to all vehicles in a certain area. As a central requirement for such safety applications, the protocol must be very robust against faults, regardless if caused accidentally or intentionally. In this paper, we examine the case of intentionally disturbances caused by attackers, i.e. the security of Geocast. We analyze weaknesses, describe potential attacks and discuss their respective effects. In a detailed study, we focus on a particularly sneaky attack, selective jamming, and show its impact on Geocast using simulations in highway and city scenarios. Particularly in highway scenarios, it is possible to disrupt Geocast flows completely using this attack.**

I. Introduction

A number of recent research projects (e.g. SafeSpot or NOW [2], [3]) and standardization efforts (e.g. Car-to-Car Communication consortium or IEEE 802.11p working group [1], [11]) address the issues of inter-vehicle communication. By enabling cars to communicate wireless with each other or with road-side equipment over short to medium distances[1] vehicles form so called Vehicular Ad-hoc Networks (VANETs). Different classes of application for VANETs are envisioned. This includes applications for traffic management, enhanced driving comfort, or car maintenance. However, the most relevant applications envisioned so far fall in the category of safety applications, where the goal is to enhance the driver awareness and reaction in critical situation by making additional information available via communication.

One classical example of such an application is an accident warning where vehicles involved in an accident start transmitting messages informing other vehicles about the precise location of the accident. If the on-board system of these other vehicles consider the message as relevant (because the vehicle is approaching that position) a warning is displayed to the driver and he can react, e.g. by slowing down the car well in advance. Such applications become especially important in situations where our natural senses are not sufficient, e.g. because the crash occurred in thick fog or behind a curve.

This raises the question, whether the intended communication range is actually sufficient. Assuming a radio range of 200 meters, a fast driving car ($120\frac{km}{h}$) will drive this distance in approximately 6 seconds. Using a rule-of-thumb formula, stopping your car from a speed of v takes you $\frac{v^2}{100}m$ for normal breaking and $\frac{v^2}{200}m$ for emergency braking. Based on a speed of $120\frac{km}{h}$ this gives you a braking distance between 72 and 144 meters. So the communication range should be sufficient to enable the driver to stop his car before hitting into the crashed cars. On top of this distance, you have to add the distance driven in the reaction time t_R of the driver which is calculated by $\frac{t_R v}{3.6}$. Assuming a standard t_R of 1 second the additional breaking distance is 33 meters, giving you a total braking distance between 105 and 179 meters. So the assumed communication distance of 200 meters is just enough to enable the driver to slow down his car without emergency breaking to stop 20 meters before the accident site.

However, additional influence factors like communication delay, bad reception conditions, distracted drivers will all badly influence the calculation, making either the communication range smaller or the reaction time of the driver longer. In the end, the application may not be able to actually warn the driver in time to prevent additional accidents. It is therefore desirable, to warn the driver as early as possible, preferably 500 or 1000 meters before the accident site. This distance is hard to achieve using omnidirectional antennas and the transmission power envisioned by [11] or even impossible in the case of unfavorable topologies like a curve with a rock face on the inner side that is blocking radio propagation.

One solution to overcome this problem is using multi-hop propagation. Vehicles receive the message and forward it to their neighbors, regardless whether they drive in the same or opposite direction. Given a certain vehicle density, this flooding process can easily reach remote vehicles at distances of one kilometer or more. In order to prevent a message from distributing arbitrarily, a mechanism restricting its reach is needed. Traditionally flooding is contained by a time-to-live counter (TTL), however in vehicular networks it is preferable to restrict the range by means of a geographic area, e.g. some specific road segments.

This leads to the concept of Geocast, which is considered

[1] according to [11] the average communication range will be in the order of 100 meters which in exceptional cases can go up to 1000 meters e.g. for emergency vehicles using directional antennas

one of the most relevant information dissemination mechanisms in VANETs. Geocast can essentially be described as a form of addressing where the destination of a packet is given by a destination region. If the sender is already within that region, Geocast can easily be implemented by geographically restricted flooding as described below. If the sender is outside the destination region, an additional transport-mechanism is needed that delivers the packet to the destination area where it can then be again flooded. So there is a basic distinction between the *transport phase* to the destination region and the *distribution phase* within the destination region.

A number of approaches to the Geocast paradigm have been proposed, the one of the first being the work of Navas and Imielinski in [12]. In his survey [7], Maihöfer categorizes the approaches into naive flooding, directed flooding and non-flooding. This categorization mainly addresses the transport phase to the destination region. In the distribution phase, i.e. the dissemination of the Geocast message within the destination region, most of the presented approaches use simple flooding.

Whereas some of the mechanisms for the transport phase, like position-based routing, have already been addressed with respect to their security challenges (e.g. in [6], [18], [16]), the effects of attacks on the distribution phase are rather unknown yet. For this reason, we focus on the security of geographically restricted flooding in this paper.

With regard to vehicular communication, the concentration on the distribution phase is also reasonable, because many applications like warning about an accident or information about a working zone do not need a previous transport to the destination region. Instead, such messages usually concern all vehicles in the proximity of the sender.

In the next section, we first describe precisely the model of the system we address and the capabilities of the attacker. On this basis, we continue with the analysis on attacks on Geocast in section III. After that, we focus on the very sneaky attack of selective jamming and examine its effects on Geocast using simulation. Finally, section V presents related work and section VI concludes the paper.

II. System and Attacker Description

Before starting to analyze the security of Geocast, we first need to concisely define the system we are examining. As a routing protocol, Geocast is typically seen as network layer implementation of the ISO/OSI reference model. Yet, for the security of Geocast, also other parts of the communication system like the application or the link layer play an important role. In addition to assumptions on the system, we also define a model of the attacker, i.e. the motivations of an attacker and the methods he can use to reach these goals. Based on that, we can detail arising problems with Geocast, when an attacker utilizes these methods.

A. System Model

In our system model, we consider ad hoc communication between vehicles, driving on streets in a city or on multi-lane freeways with large segments. Each vehicle's communication unit comprises a subset of layers of the ISO/OSI reference model, namely application layer, network layer, data link layer and physical layer. The model is based on the current status of development in the C2C-CC, but only considers the parts relevant to Geocast.

Source Identifier (SI)	Message Sequence Number (MSN)	Destination Region (DR)	Payload

Fig. 1. Schematic format of Geocast messages

The *application* is responsible to create messages based on events, e.g. when a vehicle senses a collision. Depending on the event and the vehicle's current location, the application also determines and attachs a destination region (DR) for the message. The destination region is given as a geographically shaped region like a circle or a rectangle. As motivated earlier, we assume that the originating vehicle is always located inside this destination region, i.e. only the distribution phase of Geocast is required.

As implementation of Geocast on the *network layer*, geographically limited flooding of messages is assumed. This means that a node which receives the Geocast message relays this message once, if it is currently located within the destination region given in the packet. In case the node is not located within the destination region, it discards the packet. To prevent multiple relays of the same message by one node, a duplicate detection mechanism is required. The common solution is to add a source-based message sequence number (MSN) to every packet, which is increased by the source after each packet it has sent. Thus, every packet can be unambiguously identified its source identifier (SI) and its MSN. To be able to detect packets that it has already forwarded previously, every node stores the highest known MSN per SI. If a node receives a message from SI with a lower or equal MSN, it does not forward the message again. The schematic Geocast message format is depicted in Figure1.

On the *data link layer*, we assume an implementation based on IEEE 802.11. Messages are always sent via broadcast, i.e. all nodes in transmission range are addressed and messages are not acknowledged by the receivers. Medium access is decentralized, using the CSMA/CA scheme defined in IEEE 802.11. The selection of the link layer is backed by the foreseen inter-vehicle communication system standard named IEEE 802.11p[11].

In our model, we assume to have one *physical communication* channel available. In contrast to that, the upcoming standard likely has seven channels, with at least two dedicated channels for safety-related communication [4]. But still, assuming to have only one channel is reasonable, because channel usage in the standard is subdivided according to functionality.

B. Attacker Model

As attacker, we assume a single node which is equipped with suitable radio equipment to be able to communicate with other nodes in the network. Apart from that, an attacker can act any way he wants to achieve his goals.

1) Attacker Goals: In this section, we describe goals of an attacker in relation to Geocast. This relation is fulfilled if the attacker either *a)* participates in Geocast, *b)* interferes with Geocast, or *c)* interferes with layers that Geocast relies on to achieve his goals. The attacker's goals can include:

- Global denial of service
  Targets the system as a whole, reduces general availability
- Selective denial of service
  Targets single nodes or single types of messages, reduces availability of the system for specific nodes or applications
- Information flooding/displacement
  Tries to inject and promote false information into the system

Some other typical attacker goals are not considered, as they are not applicable to Geocast when used in VANETs. For example, gaining potentially secret information is not a relevant goal, as Geocast is generally used to inform a set of vehicles unknown to the sender and is not encrypted therefore.

2) Attacker methods: An attacker may use a number of different techniques to realize his goals. The following methods are applicable within our system model.

- Forging of messages
  An attacker may create and send messages with arbitrary content and header data, at any location, time and frequency.
- Replay of messages
  An attacker may capture messages and replay them at another location or at a later time.
- Manipulation of messages
  An attacker may modify message content or header fields like the destination region before forwarding.
- Forwarding misbehavior
  An attacker may not adhere to the forwarding rules.
- Egoistic medium access
  An attacker may not respect cooperative medium access and thus monopolize the channel.
- Radio interference
  An attacker may send jamming signals

In addition, other generally applicable attack methods not specific to Geocast may be applied by an attacker. For example, impersonation is a general problem for any communication in vehicular networks. The problem is that anyone can send messages with compatible wireless equipment. Without protection, an attacker may use his slightly modified laptop, pretend to be a vehicle by selecting a valid identifier and send out messages. All other participants of the network will handle these messages as if they came from a vehicle.

	Manipulation	Replay	Forging	Forwarding misbehavior	Egoistic medium access	Radio interference
Global denial of service	X	X	X			X
Selective denial of service	X	X	X	X	X	X
Information flooding/displacement	X	X	X		X	

TABLE I
ATTACKER GOALS, AND METHODS HOW THEY CAN BE REACHED

III. SECURITY ANALYSIS

After defining the system and attacker model, the question is in which way an attacker may use the given techniques on the system to achieve his goals. Table I summarizes, which methods can be used to achieve certain goals.

A. Manipulation of messages

When manipulating messages, an attacker modifies either content or header fields of a message he received for forwarding. For Geocast security, only the header is relevant, which carries the source identifier (SI), the destination region (DR) and the message sequence number (MSN).

The effect of *manipulating the destination region* is that the message may not be received by all originally intended vehicles. In case the attacker scales down the DR, less vehicles will get informed, whereas in case of enlarged DR, much more vehicles are informed, which also leads to unwanted network load. This is particularly dangerous because flooding scales linearly: Every additional node in DR causes one additional relay transmission. Thus, if the DR is enlarged to twice the size in all Geocast messages, twice the network load can be expected on average. This additional network load when the destination region is very large and node density is high may ultimately cause a collapse of the network in the affected region.

However, as every node relays a message once, there is a chance that other nodes propagate an unmodified message first. When the attacker's version is received at his neighbors, they will detect a duplicate and therefore discard the message. On the other hand, an attacker can try to combine the manipulation with egoistic medium access and thus ensure to be the first to propagate the message. Moreover, he can also manipulate the MSN to a higher value and thus ensure that the duplicate check at the neighbor nodes will not recognize the message and thus forward it.

In addition, the success of the attack also depends on the current node topology, which is strongly related to the scenario in VANETs. When vehicles drive on highways, the node topology is almost linear, whereas it is complex in cities. Therefore, on highways less disjunct forwarding paths are available in comparison to city streets, which can make the attack more successful on highways.

Other targets for manipulations are the SI and MSN which are used for duplicate checks to prevent broadcast storms in the considered version of Geocast. As introduced before, if the attacker increases the MSN to a higher value, it achieves two effects: on the one hand, the manipulated message supersedes instances of the same message which means that the attacker is able to ensure that ”his” version is propagated throughout the destination region. On the other hand, this attack inhibits all subsequent, regular message of the same source, because other nodes already stored a higher MSN for the corresponding SI.

The feasibility of the attack depends on the predictability of subsequent MSNs of the same source node. As the name says, the subsequent MSN is usually sequentially increased, which allows nodes only to store the highest received MSN per SI.

B. Replay of messages

Capturing messages and replaying them at a later time and other location is primarily a threat on the application layer, because formerly valid messages carry outdated information when they are replayed. For example, an attacker may capture a warning about a traffic jam, replay it later and thus influence drivers to leave the highway. From the point of view of Geocast security, such a single replay is a neglectible waste of overall bandwidth. In addition, replaying the message at a location outside the DR is not useful for the attacker because surrounding nodes would immediately discard it. If the attacker replays a message within the DR, the effect depends on the time elapsed since the original message was sent. The longer the time since the original transmission, the higher the probability that the message will not be recognized as duplicate any more because all nodes have moved outside the DR. In summary, the attack would also have to modify the message to be effective, which is by definition no replay any more.

C. Forging of messages

Forging messages means that the attacker creates new, additional messages. In contrast to replay or modification, forged messages are not captured first, but assembled arbitrarily by the attacker himself. This means, that the attacker may create and send Geocast messages containing bogus information, with arbitrary SI or MSN, with a destination region whose size is only limited by the field length and at any rate. Apart from misinforming other nodes, this makes forging a very powerful attack on Geocast which can lead to overloading the system or inhibition of later messages.

Particularly overloading the system by using a large destination area and high frequency is easy to achieve with forged messages. Assume an average node density of $\rho = 10$ and a message frequency of $f = 50$ Hz. Then, the local channel load is $\rho * f = 500$ messages per second throughout the whole destination region.

But also forged Geocast messages with high MSN can cause severe damage. If the SI of the message is falsified and the message claims a high MSN, regular messages from the affected source can be inhibited. Though this attack only targets a single SI and only lasts until the topology has changed notably, sending out such an inhibition message for every new encountered node can eliminate most Geocast traffic locally.

D. Forwarding misbehavior

The Geocast forwarding algorithm executed at each node is limited to the decision whether to forward a message or not. Thus, an attacker node is only capable to achieve the opposite of the regular behavior, which means that it may illegitimately broadcast when he should not, or drop the message though he should broadcast the message according to the rationale of Geocast. The effects of such a behavior are very limited. In the first case, neighboring nodes will receive the message and discard it, as they are not addressed. Thus, the only effect is a neglectible waste of bandwidth. The effect of the second case depends on the current network topology. If the attacker is the only node to forward messages between two network partitions, then some nodes will not receive the message. However, due to high dynamics in VANETs, an attacker is not able to plan with such a topology, which makes the attack less worthwhile.

E. Egoistic medium access

The distributed coordination of access to the wireless medium allows the attacker to push in its own packets by behavior violating the standard access protocol. For Geocast, forwarding messages faster than others is not a real problem. However, the attack can be beneficial to the attacker if he has to be faster than the other nodes to propagate a modified version of a message. In this case, all other messages with the same SI and MSN will be discarded by nodes which have received the attacker's version before.

F. Radio interference

By interfering with the radio, an attacker is able to disturb communication within its transmission range. A well-known attack is jamming, for which an attacker simply keeps its transceiver sending continuously. With such a permanent jamming signal, neighbor nodes can be affected in two ways: Nodes that are close enough to the attacker that their sensing threshold is exceeded will not try to send packets because they regard the channel to be occupied. However, some of these nodes may still be able to receive packets from other nodes (outside the influence of the attacker) successfully, if the signal-to-noise ratio (SNR) at their location is large enough. Those nodes that are closer to the attacker will also not be able to receive anything due to the relatively strong signal of the attacker. In this case, the SNR of signals from outside the reachability of the attacker is not sufficient.

From the point of view of Geocast, blocking the frequency only disturbs forwarding within the transmission range of the attacker. Messages to be forwarded will not be sent due to

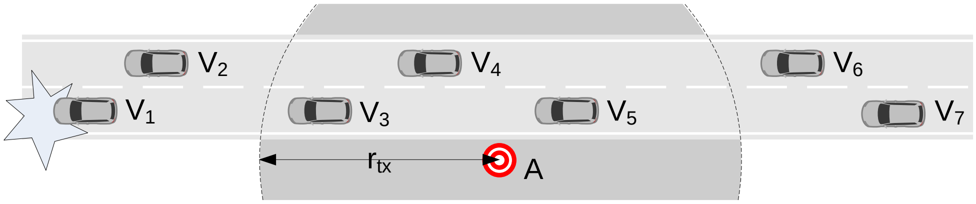

Fig. 2. Selective jamming on a highway: Complete disruption of Geocast forwarding feasible

the occupied channel, but eventually nodes may leave the influence of the attacker due to mobility and send out messages then. Thus, the scope of this attack is limited to the area where the signal of the attacker is propagated.

Instead, another attack we call ”selective jamming” has much more impact. The attack exploits the fact that Geocast messages are sent via broadcast and are therefore not acknowledged. For selective jamming, an attacker waits for messages being sent and then sends a short signal, which will interfere with the ongoing transmission and render receivers in the attacker’s vicinity unable to receive the packet successfully. This approach also enables the attacker to disrupt reception of particular messages only, e.g. after decoding parts of it during the sending. As effect of the attack, forwarding is stopped completely at the location of the attacker.

The attack is particularly dangerous because neither the sender nor any receiver in the transmission range of the attacker will be aware of the attack, since such short interference is a typical issue in wireless ad hoc networks due to the hidden terminal problem. Moreover, the attack can not be prevented because the radio hardware for the envisioned system is available for everyone.

IV. Impact of Selective Jamming

All of the described attacks can cause significant damage if they are not prevented in advance or detected and reacted accordingly (see also Table I). Though not trivial, we assume that manipulation and replay of messages can be thwarted by signatures and timestamps, and forging of messages is restricted through rate control mechanisms in this paper. Under these assumptions, one of the remaining, serious attacks is selective jamming of messages. In this section, we focus on the impact of selective jamming Geocast messages.

The danger of selective jamming derives from several reasons:

- Jamming can be done by anyone with suitable radio equipment. While communication can be restricted to valid network participants by using authentication mechanisms on higher layers, interfering with the radio is open to everyone.
- Sender is not aware of attack. During the sending of a message, it is not possible for the sender to receive on the same frequency in parallel. After sending the packet, no acknowledge is expected.
- Receiver is not aware of attack. With CSMA/CA, collisions can not be prevented due to the hidden station problem. For the receiver, the attack message will look like a collision with the Geocast packet, with the result that the Geocast message can not be decoded successfully.

An exemplary, detailed course of the attack is given along Figure 2, which depicts a part of a highway topology with seven vehicles $V_1 \dots V_7$ and the attacker A. When a Geocast message m traverses its destination region from left to right, it arrives at vehicle V_1 first. V_1 will rebroadcast m after the channel is idle and the contention backoff timer has expired. This broadcast will be received by vehicles V_2 and V_3. Then, both V_2 and V_3 also forward m the same way. Given that V_2 wins the contention first, it will rebroadcast m which is received by V_3 and V_4 this time. V_3 will discard this instance of m, because it has received it before from V_1. Next, V_3 is likely to win the contention and rebroadcasts m. However, as A is in the transmission range of V_3, A will send a short signal during V_3 is sending m, which results in collisions at the receivers V_4 and V_5. Thus, both of them have not received m. After that, V_4 tries to rebroadcast m, and A reacts also in the same way. In summary, A has completely disrupted the Geocast delivery of message m, because none of $V_5 \dots V_7$ has received m.

More generally speaking, whenever a vehicle in the vicinity of A transmits a message, A will send the short jam signal and none of all other vehicles in the range of A will be able to complete the reception successfully. This is particularly significant for highway scenarios because there are no alternate forwarding paths for Geocast messages.

In the next sections, we further confirm and investigate the effect of selective jamming using simulations.

A. Simulation Setup

As simulation tool, we use an extended version of JiST/SWANS [5]. In particular, the extensions include a network and routing module to support geographic routing and Geocast as described in the system model. Moreover, we add a mobility model to support highway scenarios, which were also used previously in the FleetNet project [10]. The simulated highway is about $14km$ long and consists of two or three lanes per direction. The number of nodes is set per kilometer and lane. To simulate the attack in a city scenario, we use the Street Random Waypoint (STRAW) model by Choffnes et al. [9]. With this model, vehicle movements are simulated

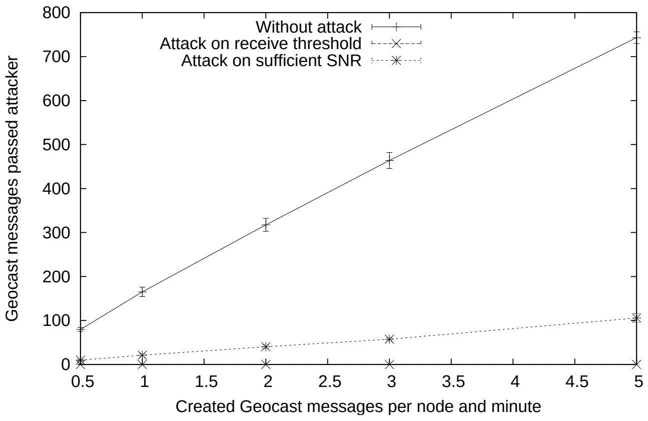

Fig. 3. Messages passing the attacker on a highway

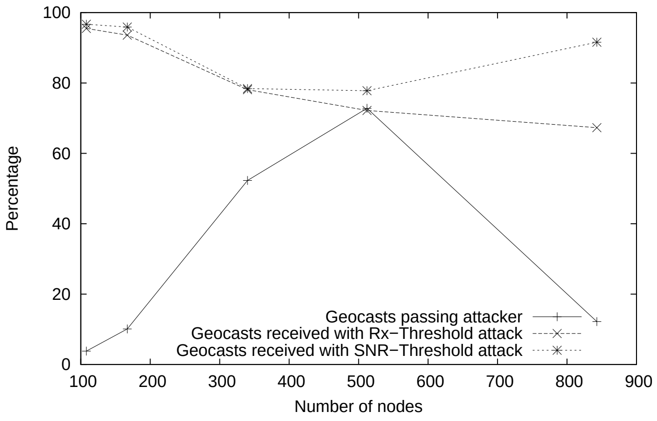

Fig. 4. Geocast message reception statisticts with different vehicle density on the highway

on a street map based on the TIGER database by the US Bureau of Census. For our simulations, we use a square area with 4km side length. As medium access and radio layers, we use an implementation of 802.11b, as it makes no difference to the envisioned vehicular system to demonstrate the attack. The attacker node itself is placed stationary in the center of the simulated field and operates a modified radio module. As introduced before, the attacker's radio is able to react either on any signals exceeding the receiving threshold or only on signals with high enough signal strength that the signal-to-noise ratio (SNR) would be sufficient to receive the packet successfully. The latter case imitates the intention of the attacker to jam not all but only packets with some special properties. For that, an attacker first has to decode a packet partly during the transmission, before he can decide whether or not to send a jam signal. Yet, in the simulation, the attacker still jams all messages. Thus, depending on the setup, there are two cases being investigated: In the first case, the attacker sends a jam signal already after a sensing a packet, i.e. when the detected signal exceeds the sensing threshold. In the second case, the attacker only sends the jam signal, if also the SNR is large enough to receive the packet.

As data traffic, the vehicles send Geocast messages with a circular destination region, where the center is the current location of the originating vehicle and the radius is randomly selected between five and eight kilometers.

In order to get statistically relevant results, each simulation configuration was executed five times.

B. Selective Jamming on Highways

The most severe impact of selective jamming is expectable in highway scenarios because there is no alternate path for Geocast messages to pass the attacker.

Figure 3 confirms this expectation. The figure outlines the number of Geocast messages that passed the attacker's location, i.e. that were originally sent left or right of the attacker, passed the attacker and were further on received on the other side. The highway in this case had two lanes per direction and on average six nodes per kilometer and lane, 340 nodes in total. Without attack and with increasing number of messages per node and minute, the number of messages that pass the attacker increases linearly, which is expectable. When the attacker sends jamming signals upon detecting a signal over the sensing threshold, no single message passes the attacker any more, regardless of the amount of data traffic. This shows that selective jamming is able to disrupt all Geocast messages when a low sensitivity threshold is used. The attack is slightly less effective when the attacker also requires to be able to decode a message first. Though it send the jam signal in every case, the attacker waits for packets with SNR that would be large enough to decode the packet. In this case, a small fraction of all Geocasts (constantly about 12% – 15%) survive the attack and manage to pass the attacker.

With these results, we show that the attack is highly effective almost independently of the current network load. Another question is whether the attack depends on the current node density. Here, the case is a little more complex, as Figure 4 shows. The problem is, that node density has also an effect on Geocast forwarding in general. One of the curves in Figure 4 lines up the percentage of Geocast messages of all generated Geocasts which pass the attackers location. Both with low and high node density, only a small percentage of all generated Geocasts pass the attackers location. Because every node generates 3 Geocast messages on average in this case, the node density is either too low or too high to complete each forwarding successfully. The reason for this is fragmentation on the one hand and frequent collisions on the other hand, which lets the Geocast forwarding to come to a halt.

The other two curves in Figure 4 show the percentage of all received Geocast messages under attack in relation all received Geocasts without attack. From this macroscopic perspective on the whole piece of highway, the results indicate that the attack is not very effective in scenarios with low density, since the comparison with and without attack almost makes no difference in received messages. Obviously, this is only due to the fact that less than 5% of all Geocasts pass the attacker because of fragmentation.

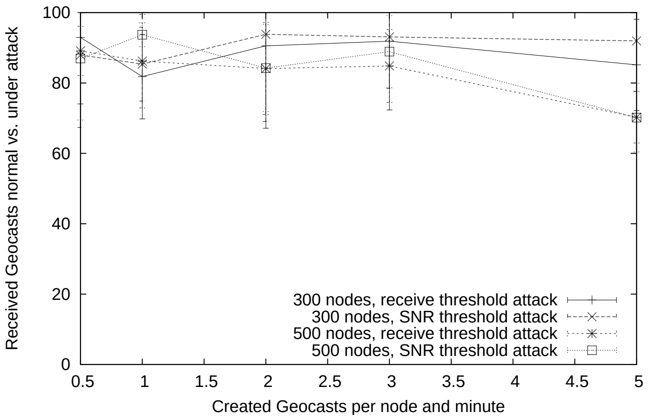

Fig. 5. Received Geocast messages under different network load, node density and attack type (city scenario)

In contrast, in the scenarios with moderate node density, the percentage of Geocasts passing the attacker reaches 50 to 70 percent. Nevertheless, the reduction in received messages is only around 20 to 30, which can be explained by the distribution area of Geocast messages. When a node on the one side of the attacker generates a message, almost any node on the same side will receive the message due to the large destination region with a radius between $5000m$ and $8000m$. Recall that the highway is about $14km$ long, which means that the attacker is roughly located at kilometer 7000. Thus, the part of the destination region of a message beyond the attacker is statistically smaller than the part on the sender's side, and therefore also contains a less of nodes that are affected by the disruption of the forwarding.

Another interesting effect in Figure 4 is that the effectiveness of the SNR-based attack decreases again with higher node density. Like the decrease in Geocast message delivery, this also derives from the high network load: Because many nodes are sending, packets can be received less frequently due to insufficient SNR, which also confuses the attacker in this case.

C. Selective Jamming in Cities

The selective jamming attack successfully can disrupt Geocast forwarding along a highway, where no physically alternate paths for the distribution are available. In this section, we consider the attack in a city scenario where street courses are more complex compared to a highway. This means that the forwarding can profit from real multi-path propagation which can make it less vulnerable against a single attacker. Figure 5 shows the percentage of received Geocast messages under attack in relation to the received messages when forwarding without attack in the city scenario.

Like before, the attacker only has influence on the nodes in its vicinity, which enables him either to prevent reception or forwarding of messages at these nodes. Depending on the local topology, missed forwarding may also cause that other nodes outside the transmission range of the attacker may not get messages.

In summary, the reduction of received messages reaches about 10 to 20 percent, which mainly depends on the used configuration. The effect mainly depends on how strategic the attackers position is. However, again the SNR-based attack is slighly less effective.

V. Related work

In [7], Maihöfer gives a good overview on Geocast mechanisms, focusing mostly on the transport phase. For the message dissemination phase basically all mechanisms rely on simple geographically restricted flooding.

Our simulation study on selective jamming showed that simple flooding does not cope well with scenarios where only few vehicles are around or where the vehicle density is high. In the first case, network fragmentation is a likely reason to stop the forwarding, and in the second case, frequent collisions cause forwarding to come to a halt.

To overcome network fragmentation, e.g. Abiding Geocast [8] has been proposed. The idea is to keep the Geocast message stable over a certain period of time, e.g. by rebroadcasting it when a new neighbor is encountered. However, this results in a even higher number of redundant transmissions than flooding alone and thus aggravates the problem in scenarios with high density. Yet, such a solution would solve the problem of disrupted Geocasts due to selective jamming. Additional work to disseminate messages in specific scenarios like on highways has been carried out be Briesemeister et al., e.g. in [14] or in [13], where the authors address the network fragmentation problem as well.

The problem with high network load of flooding in scenarios with high node density is addressed in [15]. To decrease overhead, the authors introduce several basic schemes, e.g. to select forwarders by their distance to the current sender. Another approach in [19] called Gossiping forwards messages only with a certain probability.

Regarding security of the distribution phase of Geocast, to our best knowledge, almost no work has been published so far. An initial consideration is given in [6], where the authors propose a rate threshold that limits the number of allowed messages per node. If this threshold is exceeded, messages of this not are not forwarded any more.

For the optional transport phase of Geocast, security aspects have been considered e.g. for position-based routing. Position-based routing is one alternative to implement the forwarding of a message toward its final destination region. In many position-based routing protocols, every node needs the positions of his neighbors to decide, to which neighbor to forward a given message. Thus, the position claims needs to be trustworthy, otherwise the routing can be tampered with. In [17], we proposed a trust-based position verification system for VANETs, which works only with network layer packets, i.e. does not rely on any highly accurate hardware or dedicated infrastructure.

VI. Summary and Conclusion

In this paper, we have examined the security of Geocast, i.e. the dissemination of messages by flooding within a destination region. The analysis shows that an attacker has a number of opportunities to attack the protocol with no security measures applied. Main weaknesses include the implementation of the duplicate suppression mechanism, the high network load of flooding in combination with a high frequency of messages, and the broadcast forwarding mechanism without any acknowledge.

Our study of the selective jamming attack, which specifically targets the latter weakness, shows that this is an particularly dangerous attack because anyone with suitable hardware can carry it out and because it is hard to detect for participants of the network. The simulations reveal that the attack is able to completely disrupt Geocast flows along a highway, and even cuts more than 85% of Geocasts when the attacker first needs to be able to decode the message partially.

Because many applications of vehicular communication rely on Geocast, appropriate security mechanisms need to be introduced, also with respect to the scalability problem of Geocast. Such a secure Geocast protocol will be topic of subsequent work.

In addition, some of the results may also be transferable to other forms of flooding and related multi-hop broadcast mechanisms if they do not physically transport messages.

References

[1] "Car2Car Communication Consortium," http://www.car-to-car.org/. [Online]. Available: http://www.car-to-car.org/

[2] "SafeSpot Project," http://www.safespot-eu.org/.

[3] "NoW - Network on Wheels Project," http://www.network-on-wheels.dehttp://www.network-on-wheels.de, 2005. [Online]. Available: http://www.network-on-wheels.de

[4] "Technical characteristics for pan-European harmonized communications equipment operating in the 5 GHz frequency range and intended for critical road-safety applications; System Reference Document," ETSI, Tech. Rep. TR 102 492-1, V1.1.1, 2006.

[5] R. Barr, Z. Haas, and R. van Renesse, "JiST: An efficient approach to simulation using virtual machines," *Software Practice & Experience*, vol. 35, no. 6, pp. 539–576, 2005.

[6] Charles Harsch, Andreas Festag, and Panos Papadimitratos, "Secure Position-Based Routing for VANETs," in *IEEE 66th Vehicular Technology Conference (VTC2007-Fall)*, Oct. 2007.

[7] Christian Maihöfer, "A Survey Of Geocast Routing Protocols," *IEEE Communications Surveys*, vol. 6, no. 2, pp. 32–42, 2004.

[8] Christian Maihöfer, Tim Leinmüller, and Elmar Schoch, "Abiding geocast: time–stable geocast for ad hoc networks," in *VANET '05: Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM Press, 2005, pp. 20–29.

[9] David R. Choffnes and Fabian E. Bustamante, "An Integrated Mobility and Traffic Model for Vehicular Wireless Networks," in *Proc. of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, Sep. 2005.

[10] Holger Füssler, Marc Torrent Moreno, Matthias Transier, Roland Krüger, Hannes Hartenstein, and Wolfgang Effelsberg, "POSTER: Studying vehicle movements on highways and their impact on ad-hoc connectivity," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 10, no. 4, pp. 26–27, 2006.

[11] IEEE 802.11p, "Wireless Access for Vehicular Environments – Draft standard."

[12] Julio C. Navas and Tomasz Imielinski, "GeoCast – Geographic Addressing and Routing," in *Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking (MobiCom)*, Budapest, Hungary, 1997, pp. 66–76.

[13] Linda Briesemeister and Günter Hommel, "Overcoming Fragmentation in Mobile Ad Hoc Networks," *Journal of Communications and Networks, Special Issue on Ad Hoc Networking*, vol. Band 1/3/1900, pp. 182–187, 2000.

[14] Linda Briesemeister, Lorenz Schäfers, and Günter Hommel, "Disseminating Messages among Highly Mobile Hosts based on Inter-Vehicle Communication," in *IEEE Intelligent Vehicles Symposium*, Oct. 2000, pp. 522–527.

[15] Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, and Jang-Ping Sheu, "The broadcast storm problem in a mobile ad hoc network," in *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*. New York, NY, USA: ACM Press, 1999, pp. 151–162.

[16] Tim Leinmüller and Elmar Schoch, "Greedy Routing in Highway Scenarios: The Impact of Position Faking Nodes," in *Workshop On Intelligent Transportation (WIT)*, Mar. 2006.

[17] Tim Leinmüller, Elmar Schoch, and Frank Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks," *IEEE Wireless Communication Magazine*, Oct. 2006.

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

[19] Zygmunt J. Haas, Joseph Y. Halpern, and Li Li, "Gossip-based ad hoc routing," *IEEE/ACM Trans. Netw*, vol. 14, no. 3, pp. 479–491, 2006.