An Anonymous Geocast Scheme for ITS Applications

Carsten Büttner[1,2] and Sorin A. Huss[2]
[1]*Advanced Technology, Adam Opel AG, Rüsselsheim, Germany*
[2]*Integrated Circuits and Systems Lab, Technische Universität Darmstadt, Darmstadt, Germany*

Keywords: Geocast, Vehicular Ad-hoc NETworks, Intelligent Transportation Systems, Anonymity, Location Privacy.

Abstract: We propose a novel anonymous geocast scheme for Intelligent Transportation System (ITS) applications. The main advantage of this scheme is that it allows an ITS Central Station (ICS) located in the Internet to send messages to all ITS Vehicle Stations (IVSs) subscribed to a specific ITS application and located in a certain geographic area. Thus, the messages are only distributed in the specified geographic area and not in a greater region. Furthermore, it preserves in comparison to the state of the art the privacy of the IVSs by minimizing the information about application subscriptions stored inside the network. When applying this scheme, no entity is able to exploit the ITS applications of an IVS. Moreover, no entity except the ICS provisioning the ITS application is able to exploit the IVSs subscribed to this service. We show how the proposed scheme can be integrated in mobile networks like Long Term Evolution (LTE) and networks consisting of ITS Roadside Stations (IRSs). Moreover, we compare it with the state of the art regarding the privacy of the IVSs, complexity of the scheme, scalability, supported networks, and whether the common requirements for ITS applications are fulfilled. In addition, a prototype applying the scheme for IRS networks is detailed. We demonstrate the feasibility of the proposed scheme by evaluating the implemented prototype in the context of real-world scenarios and hardware.

1 INTRODUCTION

Intelligent Transportation System (ITS) applications like a weather hazard warning, wrong way driver warning, traffic jam ahead warning, or road works warning require that the corresponding messages are distributed in a specific geographic region, called *dissemination area*, where the message is of interest for the present ITS Vehicle Stations (IVSs). The mechanism where messages are distributed in a certain geographic region is called *geocast* (Navas and Imielinski, 1997).

Given an IVS as the origin of such a message, it is typically already located within the dissemination area. Therefore, it simply distributes the message to all IVSs in communication range which are part of the Vehicular Ad-hoc NETwork (VANET) using Dedicated Short Range Communication (DSRC). These IVSs then further distribute the message in the dissemination area by means of suitable routing algorithms (Maihofer, 2004).

Besides of an IVS, an ITS Central Station (ICS) may also be the origin of such messages. An ICS can be, for example, a Traffic Center or a Service Center operated by an Original Equipment Manufacturer (OEM). It may also have access to a meteorological service or to a database of up-to-date road works information to generate the messages. Typically, an ICS is not located inside the dissemination area of the generated messages. Therefore, the messages have to be transported to the region first. This can be done by several communication technologies like mobile networks or DSRC. The IVSs located in the area may then further distribute these messages.

Some ITS applications, like the ones provided by the OEMs, are not distributed to all IVSs in the dissemination area. They may be only provided to a subset like all vehicles of a certain brand or all subscribers of a specific application. Messages of some applications may further have a commercial value and therefore require a special protection. Given that an IVS does not have a high computational power onboard, it makes sense that only the desired IVSs receive and process the messages. The dissemination area of the messages may also be dynamic. An ICS may, for example, warn about distinct weather hazards in various areas at the same time. The dissemination area may in addition change over time. Another special requirement of messages sent by ITS applica-

Büttner, C. and Huss, S.
An Anonymous Geocast Scheme for ITS Applications.
DOI: 10.5220/0005797501790189
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 179-189
ISBN: 978-989-758-167-0

tions is that they have a validity period, in which they should be also sent to each IVS entering the dissemination area.

Long Term Evolution (LTE) is the current high speed communication standard for mobile networks. Different methods exist to distribute messages via LTE to IVSs in a geographic area. However, none of them is suitable to fulfill the requirements of the outlined ITS applications: they either do not scale with the number of recipients or they are not able to automatically distribute messages to IVSs entering the dissemination area. Furthermore, the procedure becomes rather complicated when different messages have to be distributed in various frequently changing geographic areas at the same time. In addition, they do not respect the privacy of the IVSs. When exploiting DSRC, ITS Roadside Stations (IRSs) within the dissemination area and connected to the ICS may also be applied to distribute the messages to relevant IVSs. However, DSRC currently does not support the addressing of a group of IVSs as the receiver of a message. Therefore, the current mechanisms for mobile networks and DSRC are not suitable to distribute ITS messages to a group of IVSs in a given geographic area.

In this paper we propose an Anonymous Geocast scheme for ITS Applications (AGfIA), which enables an ICS to distribute an ITS message to each IVS belonging to a group and located in or entering a certain area which has been filed as a patent (Buettner and Huss, 2015). It can handle the distribution of different messages at various, even overlapping, areas at the same time. The proposed scheme works for distribution via both, mobile networks and DSRC. Moreover, it protects the privacy of the IVSs, whereas no central entity is able to track the exploited applications of an IVS. This is done by minimizing the information about application subscriptions of an IVS stored within the network. We compare the proposed mechanism theoretically with the state of the art and, in addition, we provide a prototype implementation of the scheme created and evaluated on real DSRC hardware.

The rest of the paper is structured as follows. In Section 2 we discuss the requirements of ITS applications regarding a geocast. The related work on geocasts for ITS applications via mobile networks is reviewed in Section 3. We then propose the AGfIA approach in Section 4. Afterwards, we compare it with the state of the art and present our real-world evaluation in Section 5. Finally, we conclude in Section 6.

2 REQUIREMENTS

Different kinds of ITS applications require a geocast mechanism to distribute messages. To support a wide variety of such applications, a geocast mechanism must fulfill various requirements. In the sequel we discuss these requirements.

Multiple Applications: A geocast mechanism in general introduces some overhead. In order to minimize it, a geocast mechanism should be able to handle quite different applications.

Receiver Groups: Usually an IVS does not employ all available applications. Each IVS does just subscribe to the applications it is interested in. In order to transmit the messages only to the subscribers of an application, a geocast mechanism should support the addressing of a subset of all IVSs.

Content Type: Typical ITS messages consist of small messages. Therefore, a geocast mechanism does not need to support the transmission of a huge amount of data.

Dissemination Area: Each ITS message distributed via geocast has a dedicated dissemination area. Some applications, like a weather hazard warning, might intend to distribute messages in a large area like a whole state, while others, like a particulate matter emission warning or road works warning, target only a town or just a road section. The dissemination area may also change over time. An application might further distribute different messages to various areas at the same time. In addition, these areas may overlap. Therefore, it should be possible to specify both the dissemination area and the granularity for each message.

Validity Period: Distributed messages may have a validity period of several minutes for, e.g., traffic jam ahead warnings, hours for, e.g., weather hazard warnings or even days for, e.g., road works warnings. During this validity period the ITS message should be transmitted to each IVS entering the dissemination area. Accordingly, a geocast mechanisms should support the transmission of messages to all IVSs entering the dissemination area.

Scalability: An ITS application may be used by a huge number of IVSs. Consequently, a geocast mechanism should be able to scale for a large number of receivers.

End-to-End Delay: Some ITS applications like a wrong way driver warning require a real-time delivery of the messages in the dissemination area. Therefore, a geocast mechanism should have an as small as possible end-to-end delay.

Channel Load: In order to avoid unnecessary load within the communication network, ITS messages should be transmitted in an efficient way.

3 RELATED WORK

In (Jodlauk et al., 2011) the authors propose a grid-based geocasting scheme (GBGS) for ITS applications. They divide the surface of the world into rectangles to define possible dissemination areas. The size of each rectangle is adjusted according to the number of IVSs within. When more IVSs than a threshold value are present in a rectangle, it is subdivided into two rectangles of equal size. If the number of IVSs in two neighboring rectangles drops below another threshold value, they are merged. Each IVS is aware of the rectangle it is currently in. Every time an IVS leaves a rectangle, its current position is transmitted to a so-called Geo Messaging Server (GMS). On reception, the GMS determines the new rectangle the IVS is located in and sends it back to the IVS. Therefore, the GMS is all the time aware of the position of all IVSs. An ICS aiming to sent a message to each IVS in a geographic area needs to query the GMS for all IVSs in the dissemination area first. The server then determines and returns all IVSs located in the corresponding rectangles. The disadvantage of this scheme is clearly the central GMS, which is aware of the coarse position of all IVSs and is therefore able to track them and thus may infringe their privacy. Furthermore, the scheme does not scale because each message has to be distributed to each IVS via a single unicast message. In addition, this scheme does not support the addressing of a group of IVSs in the first place. However, this feature was later on added as part of the CONVERGE project (CONVERGE, 2015). In the evaluation section we compare this scheme to our AGfIA approach.

In LTE the evolved Multimedia Broadcast Multicast Service (eMBMS) (3GPP TS 23.246, 2013) can be exploited to distribute data from a content provider to a group of recipients in predefined broadcasting areas by means of multicast. In order to apply eMBMS, each application has to register an eMBMS User Service at the Mobile Network Operator (MNO) first. An IVS aiming to exploit several applications has to register for each application separately. eMBMS was developed to download a huge amount of data or to stream audio or video data from a radio or TV station to many recipients. For this reason it is based on multicast in order to save bandwidth. Therefore, this scheme is not well-suited to distribute the rather small ITS messages. In order to support the distribution of different messages in various broadcasting areas, one eMBMS session has to be initiated for each broadcasting area, but this introduces a high complexity. Furthermore, it is not possible to have overlapping broadcasting areas. In addition, messages are not repeated automatically in order to inform IVSs entering the broadcasting area. Consequently, the messages have to be sent periodically from the content provider to the MNO, which spreads them in the broadcasting area. Obviously, this method is not very efficient. We compare this scheme with AGfIA in Section 5.

The authors of (Calabuig et al., 2014) compare the LTE unicast and eMBMS transmission modes for safety-related ITS applications. They further study the configuration of eMBMS for safety-related ITS applications. Their proposed configuration consists of a central entity which receives all messages. It is accessible by all MNOs and distributes the messages via all mobile networks covering the dissemination area. The authors also state that a new data delivery method for eMBMS is necessary to fulfill the requirements of ITS messages. They conclude that eMBMS is more efficient in terms of resource consumption when compared to unicast messages. However, this seams obvious, because less messages have to be transmitted in multicast compared to unicast. Furthermore, they do not consider multiple ITS applications with different subscriber groups.

The transmission of ITS messages via LTE and MBMS has also been studied in (Araniti et al., 2013), (ETSI TR 102 962, 2012), and (Valerio et al., 2008). However, none of them provides a solution which fulfills all requirements of ITS applications.

Three methods of cellular geocast which form the state of the art were studied in (Jodlauk et al., 2011). In the first method a central server, aiming at the distribution of a geocast message, sends an inquiry to all clients requesting their location. From the response, the server selects the relevant clients and sends the message to them. This method clearly does not scale for a large amount of clients and features a considerable delay in message delivery. The second method requires all clients to send periodical position updates to a central server which stores them in a database. When a message shall be sent to all clients in a geographic region, the central entity queries its database and sends the message to the relevant clients. This method does not suffer from the additional delay of the first method. However, it introduces some blur

on the position data, because some clients might have moved away since the last position update. In the third method the clients autonomously update their current location at the central entity when they moved a certain distance. This improves the accuracy of the positions in comparison to the second method. Nonetheless, it still has scalability problems as the first two methods. Last but not least, all these methods do not protect the location privacy of the IVSs.

4 ANONYMOUS GEOCAST

ITS applications like a weather hazard warning require a geocast to distribute relevant messages to all IVSs located in a specific geographic area. As communication technologies to perform the geocast we consider LTE for mobile networks and IRS networks for DSRC. In LTE the clients are connected to evolved NodeBs (eNodeBs) which are linked to the core network of the MNO. We assume a Mobile Network Central Station (MN CS) as part of the core network to handle all incoming ITS geocast messages. An IRS network consists of one or multiple ITS Roadside Stations, which are connected to one IRS Central Station (IRS CS). This central station handles like the MN CS for mobile networks all incoming ITS geocast messages. In case that the network consists of only one IRS, the IRS CS may also be part of this IRS. IVSs communicate with the IRS network if they are in its communication range. Both, the Mobile Network Central Station and the IRS Central Station, are connected to the Internet.

The geocast scheme introduced in the sequel may be exploited for mobile networks like UMTS and LTE as well as for IRS networks. It fulfills the special requirements of ITS applications and, in addition, protects the privacy of each IVS. The mechanisms to register for ITS geocast messages as well as the way how the messages are distributed are described for LTE and IRS networks in the sequel. Furthermore, a suitable message format for both network types, a possible usage-based billing mechanism, and an example are detailed.

4.1 IVS Registration

In order to receive geocast messages each IVS has to register for reception first. This registration is done independent of the ITS applications an IVS exploits. For the two network types different mechanisms are applied. They are detailed as follows.

4.1.1 LTE

The registration in LTE can be done like for eMBMS, where the devices join multicast groups in order to receive messages belonging to this group. In comparison to eMBMS not only one application utilizes this multicast group. Instead, all ITS applications are handled by the same multicast group. Therefore, each IVS has to join only one multicast group, independent of the number and types of ITS applications it runs. This protects the privacy of the ITS Vehicle Stations because the MNO does not learn the applications an IVS exploits. Therefore, the subscribed IVSs remain anonymous to the MNO. Furthermore, we assume a continuous eMBMS service to minimize the time overhead for setting up an eMBMS session. A time sequence diagram showing the registration scheme is depicted in the upper part of Figure 2.

4.1.2 IRS

For IRS networks no registration is necessary because the ad-hoc characteristic of the network does not need any registration. As a consequence, without a registration the operator of an IRS network is not able to track the IVSs subscribed to a certain ITS application. Therefore, the receiving IVSs stay anonymous.

4.2 Sending Messages

Whenever an ITS Central Station aims to distribute a message in a geographic area, it has to lookup the present mobile and IRS networks in the area first. To achieve this, we assume the ICS has a coverage map of all mobile and IRS networks it has a contract with. After all relevant networks have been identified, the ICS passes the message containing the dissemination area, an distribution frequency, an expiry time, and an Application ID (AID) to the central station of each network. The dissemination area defines the region in which the message shall be spread. To distribute the message also to IVSs entering the dissemination area, they are repeated at the given distribution frequency until the expiry time. The AID identifies an ITS application uniquely and is necessary for an IVS in order to determine if the particular message is relevant or not. The message distribution by the different network types is illustrated in Figure 1 and the corresponding sequence diagram in the lower part of Figure 2. We describe it in the sequel.

4.2.1 LTE

In order to handle ITS geocast messages in LTE a Mobile Network Central Station is necessary. It consists

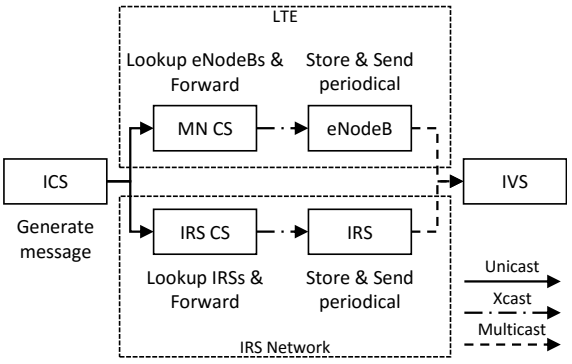


Figure 1: Message distribution in AGfIA.

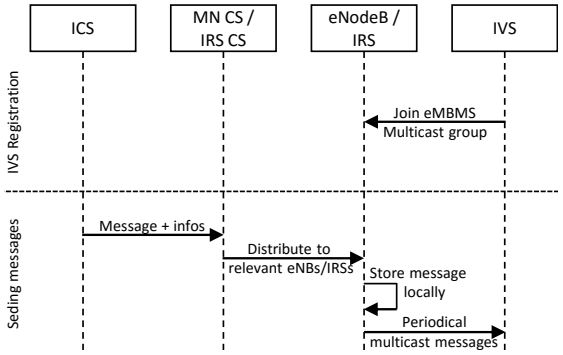


Figure 2: Time sequence diagram.

of a database, containing the position, communication range, and address of each eNodeB (eNB) within the network. Each time an ICS aims in distributing an ITS message in a certain area, it passes the messages to the MN CS. There the relevant eNodeBs to distribute the message are identified first. Then, the geocast message is forwarded to this eNodeBs by means of Xcast (Boivie et al., 2007). Upon reception the eNodeB stores the message locally. All locally stored messages are sent at the given frequency to all IVSs in communication range belonging to the ITS multicast group until they expire.

This mechanism protects the privacy of the IVSs since each IVS member of the ITS multicast group for ITS applications receives the message. Therefore, the MNO is not able to determine which IVS processes the messages and consequently can not get the applications exploited by an IVS. Furthermore, the IVS does not periodically send its position to a new central entity. This prevents tracking of IVSs.

4.2.2 IRS

For AGfIA over DSRC, the geocast messages are passed from the ICS to the IRS Central Station. The IRS CS has access, like the Mobile Network Central Station in LTE, to a database containing position, communication range, and address of each of its IRS in order to select the relevant Intelligent Roadside Stations for distribution. After selection, the messages are forwarded like in LTE via Xcast to these IRSs. There the message is stored locally and sent periodically according to the given frequency to all IVSs in communication range until it expires.

Considering that the IRS does not get any feedback which IVS in communication range processes the received message, no entity is able to determine the applications exploited by a certain IVS. Therefore, the distribution of geocast messages over IRS networks protects the privacy of the IVSs too.

4.3 Message Format

An important property of the exploited message format is that it can be applied for both communication technologies. Therefore, it is simple for the ITS central station and ITS Vehicle Station to handle the messages. The ICS needs to create only one message and can provide it to all networks. The IVS may parse the message in the same way, independent of the applied communication technology. Furthermore, an IVS may simply forward a message received by LTE to other IVSs via DSRC without the need to convert it.

We apply the GeoNetworking message format as standardized in (ETSI EN 302 636-4-1, 2014). This format was developed to exchange messages by means of DSRC between IVSs or between IVSs and IRSs. Therefore, it is well-suited for a geocast over an IRS network. We now discuss how it can be also utilized for a geocast over LTE. GeoNetworking supports unicast, anycast, and broadcast messages. For the outlined scenario it is necessary to support the addressing of a group of IVSs. Hence, we added support for multicast messages by adapting the GBC/GAC (Geographically Scoped Broadcast / Geographically Scoped Anycast) header. All GeoNetworking messages are secured by cryptographic mechanisms in order to protect their content. Besides of the adapted header aimed to support multicast, we apply the message format as denoted in (ETSI EN 302 636-4-1, 2014) and exploit the Basic Transport Protocol (BTP-A) (ETSI EN 302 636-5-1, 2014) as transport protocol.

The detailed format of the header supporting multicast is illustrated in Figure 3. The changes compared to the original GBC/GAC header are as follows. We first removed the location of the source, because it is an ICS whose location is not relevant for the receiving or forwarding IVSs. Additionally, we utilize the reserved octets to encode the Application ID (*AID*) into the message and add fields to embed the frequency

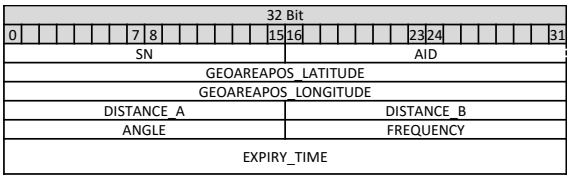


Figure 3: Detailed message format of the geographically scoped multicast.

(*FREQUENCY*) and expiryTime (*EXPIRY_TIME*) of the message. The multicast routing is added by encoding the AID into the message. Therefore, an IVS which does not support the corresponding application can drop the message without further processing. The frequency indicates how often the message shall be distributed to the IVSs in communication range by either an IVS, IRS, or eNodeB. The message is valid until the point in time encoded in expiryTime. After this point in time, all entities will drop and no longer distribute the message. All other fields are applied as in the original GBC/GAC message. The sequence number (*SN*) indicates the index of the sent packet and is utilized to detect duplicate GN packets (ETSI EN 302 636-4-1, 2014). The remaining fields are applied to describe the geometric shape of the dissemination area as defined in (ETSI EN 302 636-4-1, 2014).

This message format can be applied for both LTE and IRS networks to deliver geocast messages to a group of IVSs. When they are distributed over mobile networks, the GeoNetworking message is the payload of the IP connection. For DSRC the GeoNetworking message is also used within the Network and Transportation Layer, respectively, to deliver the message. In both cases the receiving IVS parses the GeoNetworking message by its G5 stack and checks if the message is relevant. The relevance check is done by comparing the included AID to its supported AIDs. Figure 4 illustrates the location of the GeoNetworking message in the OSI layers for LTE and DSRC, respectively. Furthermore, if an IVS receives a GeoNetworking message via LTE, it is able to redistribute it via DSRC without any modification.

4.4 Introduced Overhead

When messages are transmitted wireless, all entities in communication range receive the message. Messages are dropped at network layer when eMBMS is applied and the receiver is not part of the corresponding multicast group. In the proposed scheme, each IVS will receive the messages of all ITS applications, independent if it is subscribed to the application or not. This introduces an overhead because all received messages need to be forwarded to the DSRC stack.

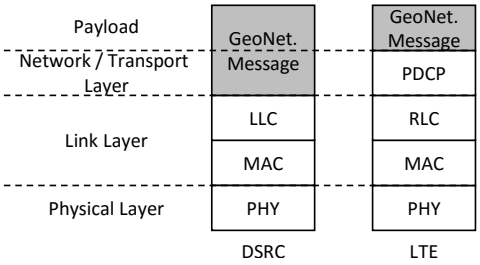


Figure 4: Comparison of the GeoNetworking message location within the LTE and DSRC layers.

There the messages are dropped if they are not relevant. Whenever messages are received via DSRC, all incoming messages are checked for relevance at network level. This analysis includes an inspection of the messages geographic region. Therefore, this check needs to be extended in order to drop messages from not supported applications at network layer.

Subsequently, there is no overhead introduced when messages are received via DSRC. For LTE each message needs to be forwarded to the DSRC stack. However, these messages are only distributed a few times per minute and have a size of less than 3000 bytes. Furthermore, it is not expected that several dozens of messages are valid in the same region at the same time. Therefore, AGfIA does not introduce a significant overhead.

4.5 Billing

For economical reasons it must be possible to bill the network usage of geocast messages. In the outlined scheme an ICS may pay a basic amount for the service provision of the operators. Furthermore, the ICS might be billed by the number of messages it sends, depending on the size of the dissemination area, sending frequency, and validity period of the messages. Therefore, the network operators do not need any information about the IVS exploiting the messages or even the number of receivers of a message. Accordingly, it is not necessary for the network operators to track the IVSs by exploiting a certain ITS application for billing. Therefore, this scheme protects the privacy of the ITS Vehicle Stations.

4.6 Example

We illustrate the advantages of the described geocast scheme by way of the example given in Figure 5. The figure shows the two hazards $Hazard_1$ and $Hazard_2$ like an icy road and roadworks. The rectangles illustrate the dissemination areas of possible warning messages. Furthermore, the eNodeBs and IRSs covering the area are depicted together with their communica-

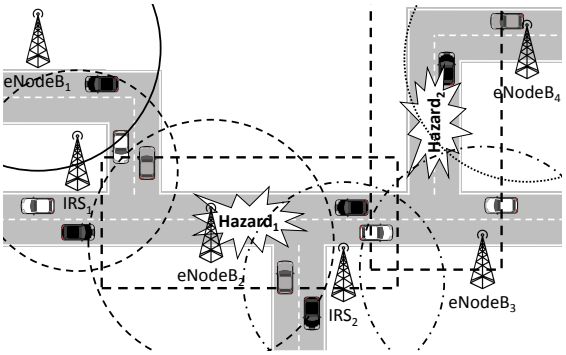


Figure 5: Message distribution example.

tion range. When exploiting the proposed scheme, only the eNodeBs and IRSs covering the respective dissemination area by their communication range distribute the message to the IVSs.

In the example IRS_1, IRS_2, and $eNodeB_2$ cover the dissemination area of $Hazard_1$, while IRS_2, $eNodeB_3$, and $eNodeB_4$ cover the area of $Hazard_2$. Since IRS_2 and $eNodeB_3$ are covering both areas, they distribute both messages. The other IRSs and eNodeBs covering only one of the areas distribute just this message. Consequently, the eNodeBs and IRSs not covering any dissemination area do not forward any message. Therefore, the messages are only distributed by the relevant eNodeBs and IRSs. Moreover, only the black ITS Vehicle Stations exploit the application warning of $Hazard_1$, while the white ones utilize the application that distributes information about $Hazard_2$. The gray ones illustrate IVSs exploiting both applications. Only the IVSs applying the corresponding application display a warning to the driver. All other IVSs discard the message. The selection of the relevant IVSs is done without having knowledge on which IVS exploits any specific ITS application at the network, nor knowing which IVSs are located within the dissemination area. Therefore, the privacy of each IVS in the dissemination area is preserved.

5 EVALUATION

For evaluation purposes we compare the privacy, complexity, and scalability figures as well as supported network types and the fulfilled ITS requirements of the proposed scheme to the grid based geocasting scheme and eMBMS. In addition, we implemented AGfIA for IRS networks and evaluated its properties on top of real-world vehicles.

5.1 Privacy

In order to compare the privacy of the different schemes, we analyze which entities are getting positions updates from the IVSs and therefore are able to track them. Furthermore, we analyze if it is possible to identify the applications utilized by a certain IVS or all ITS Vehicle Stations subscribed to a specific application.

The MNO is in all schemes able to track the IVSs. The MNO needs to know by design the location of a device to, e.g., forward a voice call or to route IP traffic to the device. Schemes like Privacy Augmented LTE as proposed in (Angermeier et al., 2013) may possibly prevent tracking by the MNO. However, they are currently not available in practice and it is therefore not possible to apply them yet. For the grid based geocasting scheme the central GMS is in addition to the MNO aware of the positions of each IVS. This is a major privacy drawback compared to the other schemes. In case that AGfIA is applied for distribution over IRS networks, a tracking of the IVSs is excluded.

An attacker aiming at identifying the applications utilized by a certain ITS Vehicle Station or all IVSs subscribed to a specific application can gain this information when eMBMS or GBGS is applied. In both schemes a local database containing the subscribers of each application exists. For eMBMS the MNO hast knowledge on which IVS is subscribed to a specific service, whereas for the GBGS the geo messaging server is aware of the applications an IVS utilizes. In AGfIA it is not possible to determine which IVSs subscribed to a certain application because this relation is not stored anywhere. It is only possible for the MNO to determine all IVSs that are utilizing ITS applications. However, this is no privacy threat at all since the MNO knows anyway by its contracts which entities are IVSs.

5.2 Complexity

To assess the complexity of the schemes we compared the procedures for application registration, geocasting a message in an additional area, utilizing an additional network to distribute the messages, and updating the position information of the IVS within the network. The results of the complexity evaluation are shown in Table 1.

In case that an ITS Vehicle Station aims to register or unregister for an application, it has to send an additional notification message to a central entity for eMBMS and GBGS. There, the relation between the IVS and application is either created or deleted. This

Table 1: Complexity evaluation.

	eMBMS	GBGS	AGfIA
Registration	Per applications	Per applications	Once
New Area	Additional session	Receiver lookup	eNB lookup
Additional Network	1 Additional message	Nothing	1 Additional message
New Position	Nothing	1 message to central entity	Nothing

Table 2: Scalability evaluation.

	eMBMS	GBGS	AGfIA
ICS to network	1 per message and receiver (U)	1 per message (U)	1 per hazard (U)
Within network	1 per router (M)	1 per receiver (U)	1 per router (X)
to IRSs / eNodeBs	1 per eNodeB (M)	1 per receiver (U)	1 per eNodeB / IRS (X)
to IVSs	1 per eNodeB (M)	1 per receiver (U)	1 per eNodeB / IRS (M)

is not necessary in AGfIA, because each IVS registers itself only once for all ITS applications and not for each application separately.

Each time an ICS intends on broadcasting a message in a new area, which happens quite often for ITS applications, an additional session has to be created if eMBMS is applied. For GBGS all IVSs in the new area have to be selected at the GMS, which may result in a considerable effort. For AGfIA only a lookup for all relevant eNodeBs and IRSs in the new area has to be made. Therefore, AGfIA has a lower complexity than both eMBMS and GBGS when messages shall be distributed in a new area.

When the message shall be distributed via an additional network, one additional message has to be sent to this network in case of eMBMS or AGfIA. For GBGS nothing has to be done, because each message is sent to each IVS individually, independent of the network it is registered at.

For eMBMS and GBGS the IVS does not need to do anything when it changes the eNodeB. Every position update is handled automatically by the mobile network. When GBGS is applied, the IVS has in addition to regularly report its position to the central GMS.

5.3 Scalability

An ITS geocast message might be sent to a large number of receivers. Therefore, it is important that the applied geocasting scheme does scale with the number of receivers. Therefore, we compared the outlined scheme with eMBMS and the GBGS regarding the number of messages the ICS needs to send to the network operator, the amount of messages within the network of the network operator, the number of messages received by the IRS or eNodeB, and the messages sent from the network to the IVSs. The results of the scalability evaluation are shown in Table 2, whereas U stands for unicast, M for multicast, and X for Xcast messages, respectively.

For eMBMS, the ICS has to pass one message to the network each time a message shall be sent to the IVSs. For the grid based geocasting scheme one message needs to be sent to the network for each IVS at each point in time a hazard message needs to be distributed. When AGfIA is applied, only one message for each hazard needs to be sent to the network no matter of how often it has to be forwarded to the IVSs. Therefore, AGfIA scales better than the other schemes mentioned. However, eMBMS performs better than GBGS in terms of scalability.

For the distribution of the messages within the network, eMBMS applies multicast, whereas almost one message is processed by each router. In contrast, one message per receiver is sent in case of GBGS. AGfIA does use Xcast to distribute the messages within the network and needs accordingly almost one message per router. Therefore, both eMBMS and AGfIA scale much better than GBGS within the distributing network.

One message is forwarded to the eNodeB or IRS, respectively, in case of eMBMS and AGfIA. When GBGS is applied, one message per receiver is sent to the eNodeBs and IRSs of the network, which results in considerably more messages compared to the other schemes.

The messages are distributed by means of multicast from the eNodeBs and IRSs of the network to the IVSs if eMBMS or AGfIA is applied. For the GBGS scheme the messages are distributed by means of unicast to each receiver, which requires more messages compared to multicast.

This evaluation shows clearly that eMBMS and AGfIA do scale better than the GBGS. In these schemes the number of messages does not depend on the number of receivers, but only on the size of the geographic area and the number of eNodeBs and IRSs

Table 3: Comparison of the fulfilled requirements.

	eMBMS	GBGS	AGfIA
Multiple Appl.	o	+	+
Receiver Groups	o	+	+
Content Type	o	+	+
Dissem. Area	-	o	+
Validity Period	o	o	+
Scalability	+	-	+
End-to-End Delay	+	o	+
Channel Load	+	-	+

located within. For AGfIA a larger message header is applied within the network to enable Xcast in comparison to eMBMS. However, AGfiA requires only one message per hazard from the ICS to the MNO, whereas for eMBMS the message has to be sent periodically to the MNO.

5.4 Supported Networks

If a scheme is able to support different kinds of networks, it may have a better coverage and therefore it may reach more ITS Vehicle Stations. Furthermore, an ICS might have a better choice of networks to utilize for message distribution. Our analysis shows that eMBMS can only be applied to LTE networks, there is no support for DSRC communication. GBGS can be utilized for transmissions over LTE and IRS networks if the IVS and IRS network do support IPv6 over GeoNetworking. In contrast, AGfIA enables the transmission over both LTE and IRS networks without the limitation on IPv6 support in DSRC.

5.5 Requirements

We evaluated which of the previously outlined requirements for ITS applications are fulfilled by the different schemes and discuss the results in the sequel. A summary is presented in Table 3.

eMBMS does fulfill the requirements for scalability, end-to-end delay, and channel load. It may also support multiple applications, receiver groups, and content type suitable for ITS applications and validity periods of messages. However, an additional effort is necessary to meet these requirement. Overlapping dissemination areas that may change over time are not supported by eMBMS, however.

The grid based geocasting scheme enables multiple applications in the first place and it was extended in to support receiver groups and is thus well-suited for ITS messages. However, the dissemination area may be in certain constellations much larger than necessary. A validity period in which messages are frequently distributed to all relevant IVSs may only be supported at an additional effort. Because it distributes all messages by means of unicast, it does not scale with the number of receiving IVSs, the channel usage is not efficient, and it features rather high end-to-end delay values.

In contrast, the advocated anonymous geocast scheme for ITS applications fulfills all outlined requirements.

5.6 Experimental Evaluation

For the real-world evaluation we implemented software to integrate the proposed scheme into IRS networks consisting of one IRS and of IVSs equipped with DSRC communication. We evaluated the software prototype in different realistic scenarios.

5.6.1 Implementation

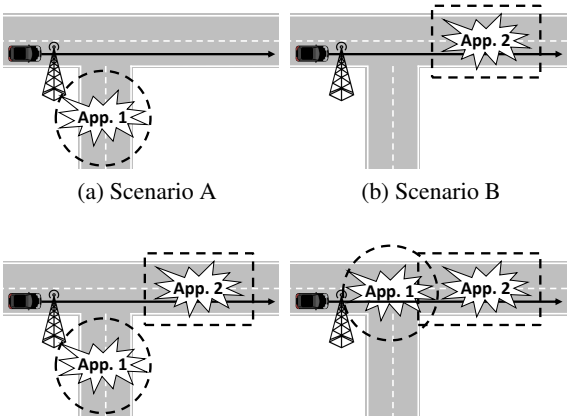
The implementation was done as part of the work documented in (Bartels, 2015) and consists of two Java programs running on the IRS and each IVS, respectively. Both programs utilize a GeoNetworking stack written in Java. The one running at the IRS CS gets as input the distribution information from an ICS. As output it distributes the message via DSRC to the IVSs in communication range. The IVS-related program takes as input the AID of the running ITS applications, the current position of the IVS, and the received messages. On reception, it parses the messages and evaluates them regarding their relevance. To consider a message as relevant, the ITS Vehicle Station has to be located inside the relevance area, it runs the corresponding ITS application, and the message at hand is not expired. The relevance area is encoded into the message and describes the actual warning region of the event. Therefore, this area is in general smaller than the dissemination area.

5.6.2 Measurement setup

Our evaluation setup consist of two IRS networks featuring one IRS each. The IRS also runs the IRS CS. Each IVS and IRS consists of an Application Unit (AU) and a Communication Unit (CCU): the AU runs the application software, whereas the CCU is responsible to send and to receive the DSRC messages. Both units are connected via Ethernet.

5.6.3 Results

Within the outlined setup we evaluated several basic and realistic scenarios. The principles of the basic



(a) Scenario A (b) Scenario B

(a) Scenario C (b) Scenario D

Figure 6: Basic evaluation scenarios.

scenarios are depicted in Figure 6. *Scenario A* consists of a message from *Application 1*, which is outside of the vehicles route, whereas in *Scenario B* the message from *Application 2* is on the route of the vehicle. *Scenario C* contains messages from different applications, where not all are on the route of the vehicle. The reception and processing of multiple overlapping messages from different applications are tested by *Scenario D*.

We ran several different tests on the basic scenarios. We varied the AIDs an IVS supports from those applications not applied in the scenario up to all AIDs of the message. To evaluate the message validity check we ran tests with valid messages, expired messages, and messages that will be valid in the future. The evaluation of the different scenarios and configurations showed that the IVSs running the particular application consider a message as relevant only in case that they are within the relevance area of the message and the message is still valid.

As an example, a realistic scenario around Rüsselsheim, Germany is depicted in Figure 7. The scenario features two IRS networks, *IRS*1 and *IRS*2, respectively. A possible route of an IVS is drawn in red aiming from Rüsselsheim city towards a motorway.

In this scenario three messages denoted as $message_1$, $message_2$, and $message_3$ are distributed to the IVSs, each with a different Application ID. The relevance area of the messages is indicated by the filled shape surrounding the message name. The bigger enclosing shape indicates the dissemination area of the messages. $message_1$ may be, for example, an icy road warning. Therefore, its shape is enclosing the icy road. The dissemination area has the same shape but covers a bigger area. $message_2$ located in the center of the city may be a notification about road closures due to a big event. To inform all IVSs reaching

Figure 7: Example of a real-world evaluation scenario.

the center, the dissemination area covers the whole city. The third message warns about a traffic jam eastbound on the highway located south to the city. Therefore, the dissemination area is only extended towards west, where the IVSs reach the traffic jam. Because of the large dissemination area of the second message, it is in reach of both IRSs and is therefore distributed by all of them. Only IRS_1 is located within the dissemination area of the icy roads warning. Therefore, only this IRS is distributing the message. For the traffic jam ahead warning only IRS_2 is located within the dissemination area and distributes the message.

This scenario clearly demonstrates the main advantage of AGfIA: Only the IRSs and eNodeBs located within the dissemination area of a certain message distribute the message. In contrast, even IRSs or eNodeBs in overlapping areas distribute all relevant messages. In addition, only the ITS Vehicle Stations exploiting the corresponding application process the message. All other IVSs drop the messages at network layer. Hence, we proved that AGfIA works well on real devices.

6 CONCLUSION

In this paper we proposed AGfIA, an anonymous geocast scheme for ITS applications. This scheme allows to send messages via various communication infrastructures to a all IVSs belonging to a specific group and being located within a certain area, without knowing which IVSs are present. Moreover, no entity is able to determine the applications exploited by a certain IVS or to identify all IVSs subscribed to a specific ITS application. Furthermore, the same message format can be applied for rather different communication technologies. We detailed on how the scheme works in terms of registration, message distribution, billing, and how the proposed message format looks like.

As data format we took the GeoNetworking message as standardized for DSRC and extended it to support multicast aimed to efficiently address a group of

IVSs. Furthermore, we compared this novel scheme regarding privacy, complexity, scalability, and the requirements of ITS geocast applications to both eMBMS and GBGC. Additionally, we implemented the scheme for DSRC, set up experimental IRS networks, and evaluated the prototype software on top of real IVSs. The presented results show that the AGfIA system is well-suited for an efficient and at the same time privacy-preserving distribution of ITS messages to a group of ITS Vehicle Stations located within a certain area.

ACKNOWLEDGEMENT

This work was funded within the project CONVERGE by the German Federal Ministries of Education and Research as well as Economic Affairs and Energy.

REFERENCES

3GPP TS 23.246 (2013). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (Release 12).

Angermeier, D., Kiening, A., and Stumpf, F. (2013). PAL - Privacy Augmented LTE: A Privacy-preserving Scheme for Vehicular LTE Communication. In *Proceeding of the 10th ACM International Workshop on Vehicular Inter-networking, Systems, and Applications*, VANET '13.

Araniti, G., Campolo, C., Condoluci, M., Iera, A., and Molinaro, A. (2013). LTE for vehicular networking: a survey. *IEEE Communications Magazine*.

Bartels, F. (2015). Senden und Empfangen von C2X-GeoMulticast-Nachrichten. Technical report, Rhein-Main University of Applied Sciences.

Boivie, R., Feldman, N., Imai, Y., Livens, W., and Ooms, D. (2007). Explicit Multicast (Xcast) Concepts and Options. RFC 5058.

Buettner, C. and Huss, S. A. (2015). Verfahren zum Verbreiten einer Nachricht. Patent application, DE 102015009599.4.

Calabuig, J., Monserrat, J., Gozalvez, D., and Klemp, O. (2014). Safety on the Roads: LTE Alternatives for Sending ITS Messages. *IEEE Vehicular Technology Magazine*.

CONVERGE (2015). Architecture of the Car2X Systems Network. Deliverable D4.3.

ETSI EN 302 636-4-1 (2014). Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality.

ETSI EN 302 636-5-1 (2014). Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol Functionality.

ETSI TR 102 962 (2012). Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS).

Jodlauk, G., Rembarz, R., and Xu, Z. (2011). An Optimized Grid-Based Geocasting Method for Cellular Mobile Networks. In *Proceedings of the 18th ITS World Congress*.

Maihofer, C. (2004). A survey of geocast routing protocols. *IEEE Communications Surveys Tutorials*.

Navas, J. C. and Imielinski, T. (1997). GeoCast - Gographic Addressing and Routing. In *Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking*, MobiCom '97.

Valerio, D., Ricciato, F., Belanovic, P., and Zemen, T. (2008). UMTS on the Road: Broadcasting Intelligent Road Safety Information via MBMS. In *Proceeding of the IEEE Vehicular Technology Conference*, VTC Spring 2008.