Chapter 8
Forwarding in VANETs: GeoNetworking

Andrea Tomatis, Hamid Menouar, and Karsten Roscher

Abstract Nowadays connectivity in the vehicles is becoming the base to enable safety, traffic efficiency, and infotainment applications. These applications require to exchange information with specific geographical locations. After a decade of research and standardization activities, a dedicated technology to support forwarding in Vehicular Ad-hoc Network (VANET) called GeoNetworking has been completed in Europe. This chapter will provide an overview of GeoNetworking features and functionalities describing geographical addressing and geographical forwarding in an easy and understandable way for both technical and non-technical readers.

Keywords VANET • GeoNetworking • Geocast • Geounicast • Geobroadcast • Media-dependent • Media-independent

8.1 Introduction

Vehicular applications often require communication among vehicles located within a specific geographical area or at specific geographical locations. For instance, if there is a traffic jam or a collision, all vehicles heading towards this traffic jam should be warned. On the other hand, for the vehicles moving away from this area, this information is not relevant anymore. This is where GeoNetworking could offer great support to these applications.

A. Tomatis (✉)
Hitachi Europe - Information and Communication Technologies Laboratory (ICTL), Ecolucioles B2, 955, route des Lucioles, 06560, Valbonne - Sophia Antipolis, France
e-mail: andrea.tomatis@hitachi-eu.com

H. Menouar
Qatar Mobility Innovations Center - QMIC, Qatar Science & Technology Park, Doha, Qatar
e-mail: hamidm@qmic.com

K. Roscher
Fraunhofer Institute for Embedded Systems and Communication Technologies ESK, Hansastraße 32, 80686 Munich, Germany
e-mail: karsten.roscher@esk.fraunhofer.de

C. Campolo et al. (eds.), *Vehicular ad hoc Networks*,
DOI 10.1007/978-3-319-15497-8_8

A simple definition of GeoNetworking is: *a set of Network Layer functionalities that uses geographical information of the involved vehicles to enable ad-hoc communication without the support of fixed infrastructure.* In other words it provides wireless ad-hoc communication among vehicles and to roadside units. GeoNetworking is part of the ITS Station reference architecture [1] and supports ITS applications for safety, traffic efficiency, and infotainment with network functionalities. In particular, it offers broadcasting of safety related messages in a certain geographical destination region, using multi-hop communication if needed and unicast communication for Internet applications [3].

GeoNetworking uses the geographical position of vehicles and roadside units to disseminate the information. GeoNetworking has two main functionalities, geographical addressing and geographical forwarding which will be depicted in this chapter.

GeoNetworking has been standardized by ETSI TC ITS in a multi-part standard series which describes the specific details of the network layer. In particular, two major documents have been published:

- Media Independent [4]: This document specifies the principal functionalities of the network layer which are independent from the media used by GeoNetworking.
- ITSG5 Media Dependent [5]: This document specifies the functionalities which are related to ITSG5 media (e.g., DCC, etc.).

The following sections introduce the GeoNetworking functionalities as defined in the ETSI Standards in an easy to understand way for both technical and non-technical readers.

At first, the base of routing is described in Sect. 8.2. In Sect. 8.3 the different addressing techniques used in GeoNetworking are described. Section 8.4 follows describing the principles of the position-based forwarding. The protocol functionalities of GeoNetworking are deeply described with examples in Sect. 8.5. Finally the security aspects, the duplicate packet detection, and the GeoNetworking special features are, respectively, described in Sects. 8.6–8.8.

8.2 Routing Based on Positions

Routing or *forwarding* in a communication network is the process of transporting information from a source towards its destination. Forwarding usually involves intermediate nodes that relay data packets on behalf of the source. It is the task of a routing protocol to find the correct path to reach the destination.

Most routing protocols leverage information about the topology of the network to calculate a path between a source and a destination. The topology is defined by direct communication links between peers as well as the properties of such links. However, the topology of vehicular ad-hoc networks is highly dynamic. Thus, links often exist only for a brief moment and can undergo significant fluctuations during their lifetime. Using link state information to determine end-to-end paths

under these conditions requires a massive overhead to distribute link state updates. Furthermore, discovery of an entire path might not be feasible at all if the process takes longer than the average lifetime of the communication links.

Shifting forwarding decisions for each communication hop (intermediate forwarder) to the individual nodes rather than calculating an entire path at once can avoid such problems. Nonetheless, a globally available metric defining how to *get closer* to the destination is required for the routing process to converge. Absolute geographic positions are an ideal basis for such a metric. This leads to a simple requirement: Each node must have the ability to determine its current geographical position. However, since modern vehicles are usually equipped with navigation devices it can be assumed that they have the ability to locate themselves using GPS, GLObalnaya NAvigatsionnaya Sputnikovaya Sistema (GLONASS) or similar technologies with reasonable accuracy.

Based on position information several routing algorithms have been proposed. Since they offer distinct properties and trade-offs between reliability and efficiency, ETSI GeoNetworking offers the choice between different algorithms. The basic principles of these algorithms are described in Sect. 8.4. An additional benefit of a position-based networking approach is a simple and efficient implementation of packet delivery based on the current location of potential receivers. This leads to new features in terms of addressing which are the topic of Sect. 8.3.

8.3 Addressing

Addressing specifies the intended recipients of a data packet. Four different addressing schemes can be identified in most modern networks:

- **Unicast** packets are delivered to a single, specific node uniquely identified by a destination address.
- **Broadcast** packets are delivered to all hosts in a certain network.
- **Anycast** addressing is used to send data to at least one member of a distinct group sharing common criteria.
- **Multicast** packets, on the other hand, are sent to all members of a group.

However, GeoNetworking uses slightly modified approaches to cope with the special requirements of information dissemination in vehicular safety and traffic efficiency applications.

8.3.1 GeoUnicast

GeoUnicast addresses a single and specific node. This is similar to the common unicast, e.g. in IP-based networks. However, in addition to a unique node identifier the position of the node is used to route the packet towards its destination. Figure 8.1 provides an example. If the current location of the destination is not available at the source node, a *Location Service* is used to gather this information.

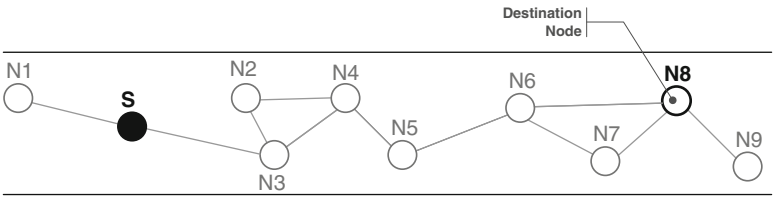

Fig. 8.1 GeoUnicast example

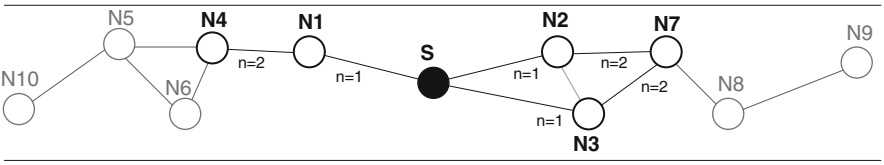

Fig. 8.2 Topological Broadcast example with $n = 2$

8.3.2 Topological Broadcast

Topological Broadcast addresses all nodes that can be reached with at most n forwarding operations (hops). This process is similar to the common broadcast with added control over the dissemination distance (in terms of hops). Figure 8.2 illustrates the process for $n = 2$. Packets that are forwarded only once ($n = 1$) are referred to as SHB.

8.3.3 GeoBroadcast/GeoAnycast

GeoBroadcast and GeoAnycast address, respectively, at least one (anycast) and all (broadcast) nodes within a specific destination area. This destination area is defined and provided by the upper layer generating the request. The source of the packet may or may not be within the destination area. Figure 8.3 illustrates communication targeting all nodes within a circular destination GeoArea.

There are similarities between GeoBroadcast/GeoAnycast and common multicast/anycast operations if all nodes in the destination area are considered to be part of a multicast or anycast group. However, groups in IP-based networks are either predefined (with a predefined address) or explicitly formed using some kind of subscription model because they are intended to be used for multiple transmissions over a longer period of time. Groups in GeoNetworking are formed implicitly based on the current location of involved nodes, which is often very dynamic. In most cases they are valid only for a single packet.

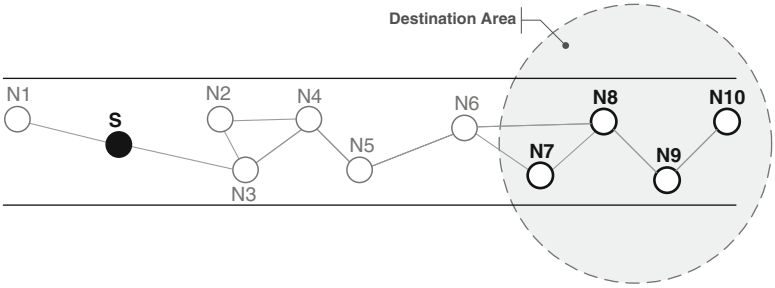

Fig. 8.3 GeoBroadcast example

8.4 Basic Principles of Position-Based Forwarding

Depending on the addressing scheme there are different phases of the forwarding process with distinct characteristics and specific algorithms. Topological Broadcast packets are forwarded with a limited *flooding* approach using simple re-broadcasts as long as the maximum number of hops is not reached. GeoUnicast requires forwarding of a packet towards a specific location, more precisely the location of the destination. This process is called *line forwarding*. GeoAnycast and GeoBroadcast use line forwarding as well to route a packet towards a node in the destination area if the sender is not located within that area. In case of a GeoBroadcast different flooding algorithms are used to efficiently distribute the information once the packet is in the destination area. Table 8.1 summarizes the different phases for each addressing type.

For line forwarding there are two basic approaches: explicit selection of a next hop by the current forwarder (sender-based) or implicit selection of a forwarder among all candidates through a decentralized coordination function (receiver-based). The former is used by Greedy Forwarding, the latter is the basis for Contention-Based Forwarding (CBF).

CBF—or variations of it—are also used to improve the flooding efficiency for geo-broadcast packets within the destination area. More information can be found in [11].

In addition to the forwarding from node to node, *store-and-forward* mechanisms can be used to temporarily buffer a packet for which forwarding is not possible at the moment. The buffer contents are reevaluated whenever the context of the node changes, e.g. a new neighbor was detected or an existing neighbor moved into a better position.

Table 8.1 Forwarding phases for different addressing schemes

Addressing	To destination	Within area
Topological Broadcast	–	Flooding (simple)
GeoUnicast	Line forwarding	–
GeoAnycast	Line forwarding	Broadcast once if source is within area
GeoBroadcast	Line forwarding	Flooding (simple or advanced)

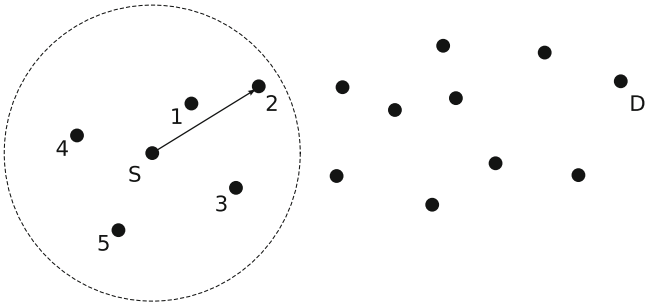

Fig. 8.4 Greedy forwarding example

8.4.1 Greedy Forwarding

Greedy forwarding was introduced as part of Greedy Perimeter Stateless Routing (GPSR) [10]. In greedy forwarding each node that needs to forward a packet explicitly selects the next hop among all its known neighbors. That requires up-to-date location information from surrounding nodes. This information can be distributed via periodic heart beats (beacons) or added to sent data packets. Applying the *most forward within radius* rule the peer closest to the destination is selected. This approach maximizes the distance progress per hop and thus results in fewer forwarding steps and efficient usage of the wireless channel.

Figure 8.4 illustrates the process with an example: The source node S wants to send a packet to the destination D. Within its transmission range there are five other nodes 1–5 with node 2 being the closest to the destination. Thus node 2 is selected and the packet sent to it. On reception of the packet the same process for selecting the next forwarder is repeated until the destination is reached.

The appeal of greedy forwarding lies in its simplicity and efficient use of the communication channel. Nevertheless, the selection of a specific node can have negative consequences for reliability. If the designated next hop moved out of transmission range or disappeared completely, data packets might get lost. This can partly be avoided with additional packet buffering and recovery strategies for transmission failures on the network layer but retransmissions increase packet latency in any case.

8.4.2 Contention-Based Forwarding

CBF [8] aims at improving reliability by leveraging multiple forwarding candidates for each step. It belongs to the opportunistic routing approaches where the receiving node decides whether it should continue forwarding or not.

Packets are sent using the broadcast mechanism of the wireless medium. Every node that received the packet checks whether it is closer to the destination than the previous forwarder in which case it is considered to be a forwarding candidate. The location of the previous transmitter is required for this process. It can either be piggy-backed on the data packet itself or derived from periodic information about neighbor positions similar to greedy forwarding.

For each step multiple forwarding candidates need to be coordinated to avoid concurrent access to the wireless channel as well as unnecessary repeated transmissions of all candidates. This can be done without additional communication overhead by applying a distinct forwarding delay at each node before sending the packet again. This delay is also called *contention timer*. If a forwarding candidate receives the packet a second time while the timer is still running it refrains from sending the packet itself since it has already been forwarded by someone else.

The delay time for each node is inversely proportional to the distance progress over the previous forwarder [8]. Thus, the node with the greatest progress has the shortest delay and tries to forward the packet first. This leads to an efficient channel usage since the distance covered with each forwarding step is maximized.

Figure 8.5 illustrates the process with an example: Source node S wants to send a packet to node D. In transmission range are five nodes that will receive the packet broadcast. Nodes 4 and 5 are farther from D than S and are therefore no candidates for forwarding. Nodes 1–3 provide progress over S. Each of them calculates its contention timer value t, buffers the packet, and waits for the determined time. Since node 2 is closest to D it has the shortest delay and will rebroadcast the packet on expiry of its timer after 10 ms. Nodes 1 and 3—still waiting—also receive the transmission of node 2, cancel their timers, and stop forwarding the packet.

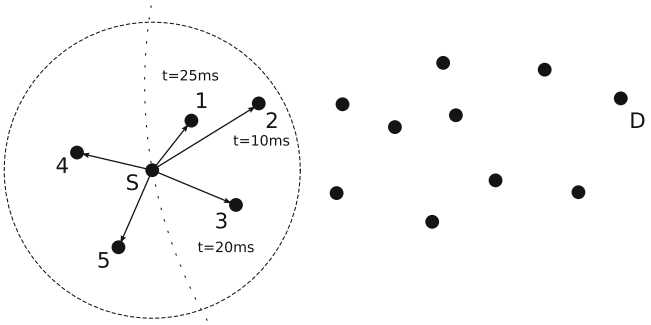

Fig. 8.5 Contention-based forwarding example

CBF offers increased reliability over the greedy approach through multiple forwarders at the cost of higher latency and increased channel usage. The individual delays of each step accumulate over the entire path. An effect that obviously gets more severe with increasing distance between source and destination. Algorithms with explicit selection of a next hop are guaranteed to use only a single transmission for each forwarding step.[1] CBF, on the other hand, can cause multiple transmissions on the wireless channel if at least two candidates are not within each other's communication range. In such cases the suppression of additional forwarding attempts fails and the packet is sent a number of times.

8.5 Protocol Functionalities

This section presents the main GeoNetworking functionalities of an ITS Station as defined in the ETSI TC ITS Specifications [4, 6] in an abstracted and easy way to understand.

8.5.1 GeoNetworking Beacon

In GeoNetworking each mobile node has to periodically inform neighbors about its presence by periodically broadcasting a specific packet called GeoNetworking Beacon.

Based on GeoNetworking Beacons received from the neighbors, a node builds a Location Table which can be consulted at any time to know the neighboring nodes and their locations. The Location Table is populated not only with information about direct neighbors, i.e. those that are located within one hop communication range and from which beacons are received, but also with farther neighbors, i.e. those located at two-hops distance and more. The farther neighbors can be added to the Location Table if a GeoNetworking Packet is received from them through multi-hop communication.

8.5.1.1 Scenario

Figure 8.6 shows a representative example of a GeoNetworking Beacon exchange and Location Table update. In the shown example, a node is surrounded by direct neighbors (N1–N3) as well as non-direct neighbors (N4–N8). Direct neighbors are inserted into the Location Table of S as soon as a beacon is received from them, while non-direct neighbors are added to the Location Table of S only if a GeoNetworking Packet that contains the location information of that neighbor is received.

[1] Retransmissions not taken into account.

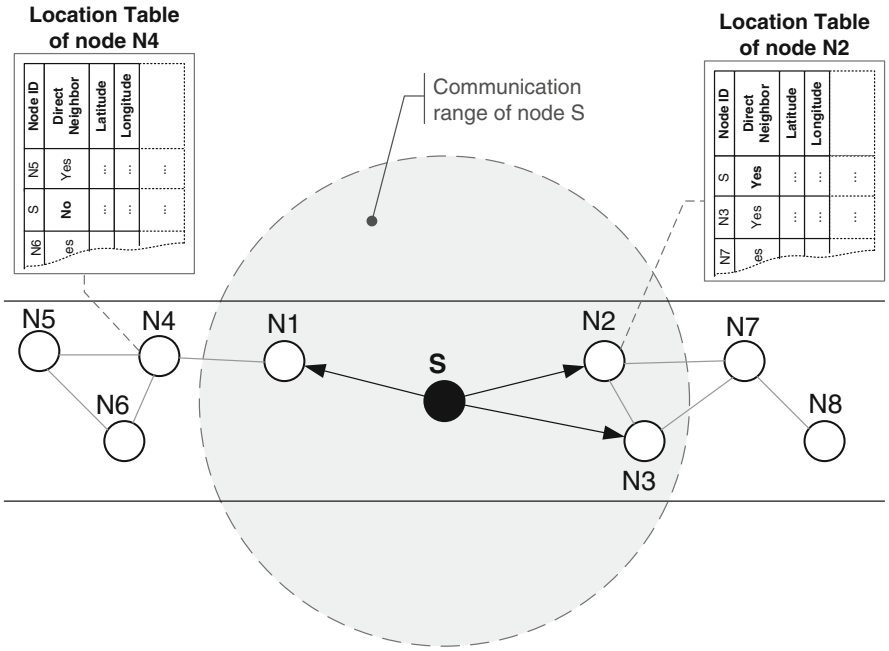

Fig. 8.6 GeoNetworking Beacon exchange and Location Table update

8.5.1.2 Protocol Operations

Before digging into the details of the GeoNetworking Beacon protocol operations, it is important to understand the data structure of the GeoNetworking packet. A GeoNetworking Packet is composed of three parts as shown in Fig. 8.7, where the first two parts are always included, while the last part is added only when needed. The fields included inside the basic header can be changed by the forwarding nodes, while the fields in the common header are set at the beginning by the originator node and then remain the same till the packet reaches its destination. This is important to make the cost of the security as low as possible, where the common header needs to be signed only once at the originator node, and then remains unchanged throughout the forwarding path.

The Basic Header is a set of information fields which is inserted in every GeoNetworking packet, and it expresses the basic information about the packet as follows:

- **Version**: expresses the version of the utilized GeoNetworking protocol.
- **NH**: stands for Next Header and it expresses the type of the header which comes after the basic header. Here in case of Network Beacon, NH indicates Common Header as next header.

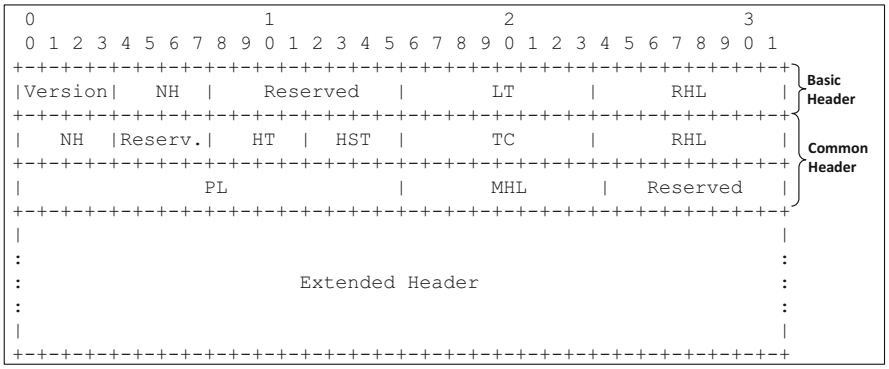

Fig. 8.7 The structure of a GeoNetworking packet

- **LT**: stands for Life Time and it expresses the time a packet is maintained alive till it reaches its destination.
- **RHL**: stands for Remaining Hop Limit and it expresses the remaining number forwarding hops. It is decreased by one at each forwarder.

The Common Header is another set of basic information fields which is also inserted in every GeoNetworking packet to express common information about the packet. These information fields are set initially by the originator node and remain unchanged till reaching the destination. The common header information fields are presented briefly as follows:

- **NH**: stands for Next Header and it expresses the type of the header coming next i.e. the type of protocol at the upper layer (Transport Layer).
- **HT**: stands for Header Type and it expresses the type of the GeoNetworking header as well as protocol, e.g. Network Beacon, GeoBroadcast, GeoUnicast, etc.
- **HST**: stands for Header Sub-Type and it is used to express the sub-type of the GeoNetworking header as well as protocol, e.g. to indicate Single-Hop or Multi-Hop Communication protocol under Topology Scooped Broadcast communication.
- **TC**: stands for Traffic Classes and it expresses upper layer requirements, e.g. in terms of priority.
- **Flags**: is partially used to express whether the source node is mobile or not.
- **PL**: stands for Payload Length and it expresses the length of the upper layer payload in bytes. Here in case of GeoNetworking Beacon it is set to zero as there is no payload attached.
- **MHL**: stands for Maximum Hop Limit and it expresses the maximum distance in terms of hops that the packet can be forwarded away from the source node. In the case of a GeoNetworking Beacon packet, the field MHL is always set to 1 as the beacon packet must not be forwarded.

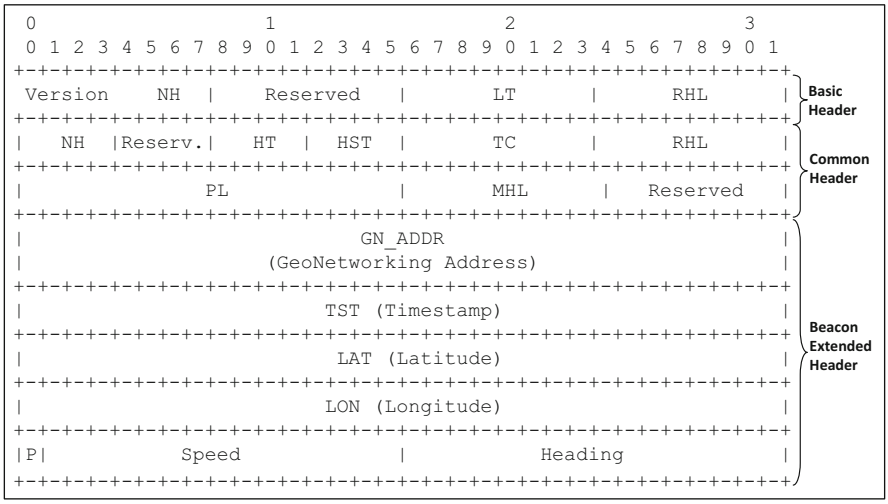

Fig. 8.8 Packet structure and headers of the GeoNetworking Beacon packet

The GeoNetworking Beacon includes a Basic Header as well as a Common Header, followed by an extended header as shown in Fig. 8.8, and which provides the unique identifier of the sender node and information about its most recent location.

Each node in the network has to inform other nodes in its surrounding about its presence in the network. To achieve this, each node creates a GeoNetworking Beacon packet as shown in Fig. 8.8, and fills the necessary information before transmitting it out. Among the necessary information, the node has to fill the GN_ADDR field with its own GeoNetworking Address. This address represents the principal identifier of the node and it contains the following information:

- **M**: this field allows to distinguish between a manually configured station and a station which is automatically configuring its address. For example, in case the pseudonyms are used see Sect. 8.6 for more details.
- **ST**: this field identifies the ITS Station type as described in [7].
- **SCC**: stands for ITS Station Country Code. Currently this field is not used.
- **MID**: this field represents the Link Layer address of the principal radio device or alternatively it contains the pseudonym (see Sect. 8.6 for more details).

Additionally the node has to fill the remaining fields in the extended header with the most updated information about its location and the Timestamp (TST) field is set with the Timestamp representing the time when the location information has been calculated.

The Beacon is sent with updated location information every few seconds. As the same information, i.e. GN_ADDR and node location, is also included in the extended header of other GeoNetworking packets, e.g. Single-Hop Broadcast, there is no need to transmit the Beacon packet if another packet containing the GN_ADDR and location of the node has been transmitted before the expiry of the Beacon timer.

All nodes located within the communication range of the sender should receive its GeoNetworking beacons. And when receiving a GeoNetworking beacon packet, or any other GeoNetworking packet which contains the GN_ADDR and location information of the node from which the packet has been received, a receiver node decodes that packet and extracts the information about the sender (i.e., GN_ADDR and Location). This information is inserted in a local location table, which lists the GeoNetworking nodes present in the surrounding. Each node listed in the local location table is flagged either as a direct or an indirect neighbor. When receiving a GeoNetworking Beacon from a node, that means this node is a direct neighbor, and therefore when inserting it in the location table it is labeled as a direct neighbor.

8.5.2 Single-Hop Broadcast

SHB is a simple and basic broadcast protocol, and it is a sub-set of the Topological Broadcast protocol as defined in Sect. 8.5.3. In SHB, the transmitted packet is never forwarded by the receivers, and therefore it reaches only neighbor nodes within the communication range of the sender. Such a broadcast protocol can be used by safety applications that require fast information dissemination in the surrounding space.

8.5.2.1 Scenario

Figure 8.9 shows an example where a node S uses SHB communication to disseminate information to its neighbors. The SHB dissemination reaches only those nodes that are located within the communication range of node S, i.e. nodes N1–N3.

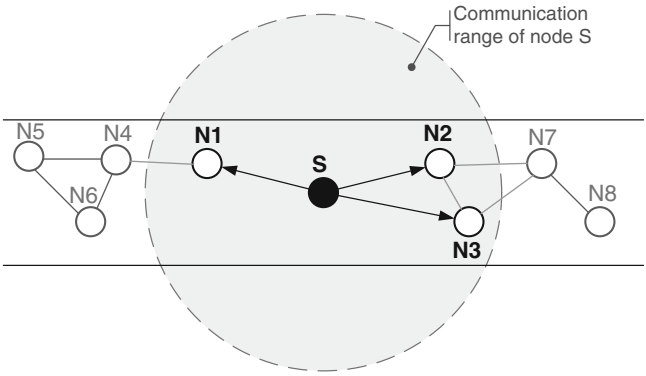

Fig. 8.9 Single-Hop communication scenario

8.5.2.2 Protocol Operations

The size as well as the content of the SHB packet has been reduced as much as possible as shown in Fig. 8.10. The SHB packet includes a basic header and a common header, followed by an extended header which includes only information about the sender, i.e. GeoNetworking Address and Location of the sender.

When the sender node receives a payload from upper layer to transmit throughout the network using an SHB scheme, an SHB packet (as shown in Fig. 8.10) is created and filled with the necessary information as follows:

- The GN_ADDR field is set with the GeoNetworking address of the sender node,
- the LAT/LON fields are filled with the most updated location coordinates of the sender node,
- the TST field is set with the Time Stamp (in milliseconds) by when the most updated location coordinates of the sender node have been calculated, and finally,
- the Speed and Heading fields are filled with the sender movement Speed and Heading, respectively. The field P is used to express whether the location coordinates of the node are accurate enough or not.

Four bytes have been reserved at the end of the SHB extended header, to be used in the future by media dependent functionalities (see Sect. 8.8.3).

Whenever a node receives an SHB packet, the node decodes it first and then checks if the packet has not been already processed previously. This duplicated

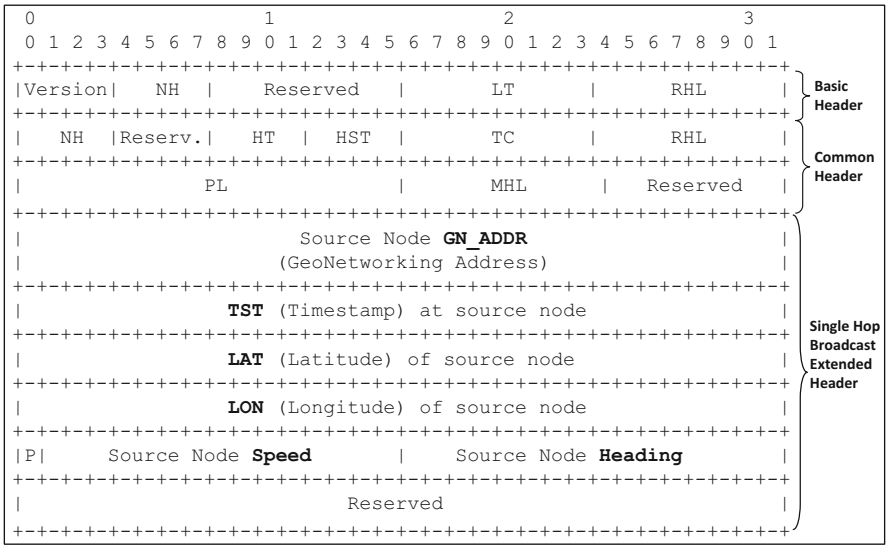

Fig. 8.10 Packet structure and headers of the GeoNetworking SHB packet

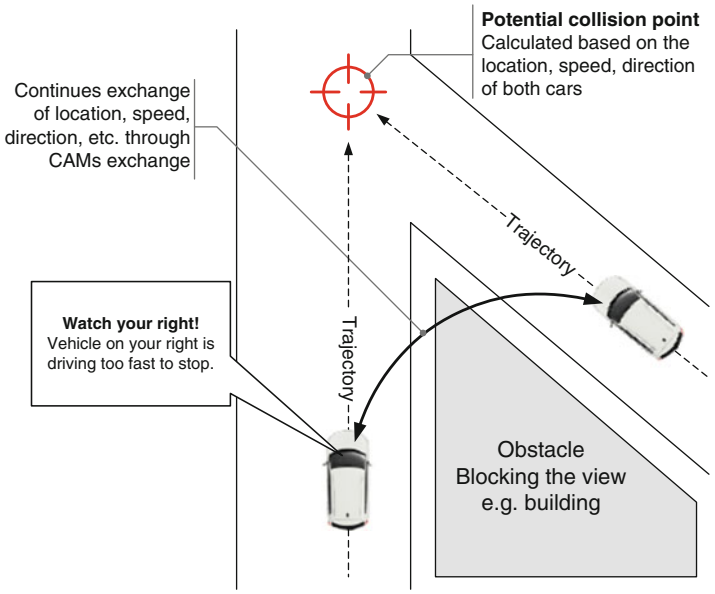

Fig. 8.11 Collision avoidance use-case enabled by continuous exchange of CAMs through GeoNetworking SHB. communications

packet check is achieved by comparing the GN_ADDR and acTST fields in the received packet against local information about packets that have been received and processed in the past (see Sect. 8.7).

8.5.2.3 Example of Usage

Figure 8.11 shows a typical use-case example where SHB communication is used to avoid collisions at an intersection. Such use-case is enabled based on the continuous exchange of the location, speed and direction of the cars through the cooperative awareness message (CAM).[2] The CAM is continuously and periodically broadcasted by each car using SHB.

8.5.3 Topological Scoped Broadcast

When tackling short range wireless communication systems and dealing with a limited communication range, any packet that needs to be transmitted beyond the communication range has to fly throughout multi-hop communications, where intermediate nodes (called also relays) forward the packet till reaching its destination.

[2] See Chap. 5 for more details about CAM messages.

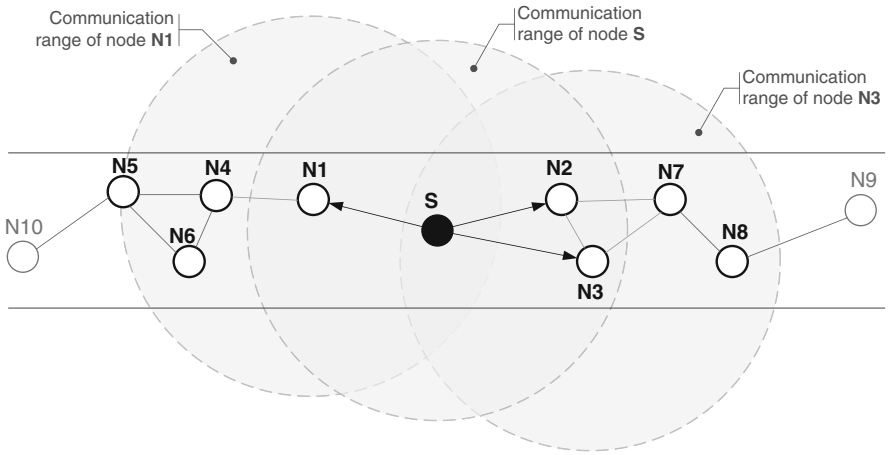

Fig. 8.12 Topological Broadcast (two hops) scenario

Topology Broadcast is well known not only in the vehicular communication field, but also in the ad-hoc communication field in general as it has been one of the first and basic forwarding schemes adopted in the community.

8.5.3.1 Scenario

Figure 8.12 presents the Topological Broadcast scenario through a 2-hop Topological-Broadcast example. In the shown example, a node S initiates a 2-hop Topological Broadcast dissemination, by transmitting a Topological Broadcast packet to all nodes within its communication range, i.e. nodes N1–N3. As the communication is intended for 2-hops distance, the packet is forwarded once by selected forwarders among the direct neighbors, to reach the second hop neighbors, i.e. nodes N4–N8.

8.5.3.2 Protocol Operations

Whenever a node receives a payload from upper layer to disseminate within a defined number of hops, a Topological Broadcast scheme is triggered and a Topological Broadcast packet is created (as shown in Fig. 8.13). The necessary information is then filled in the Topological Scoped Broadcast (TSB) packet similar to SHB as explained previously, i.e. GeoNetworking address and location fields in the Extended header with the sender information. As packets forwarding is allowed in Topological Broadcast, a same packet might reach a destination or an intermediate node through different neighbors (i.e., different forwarders). In such a case, only the very first packet is processed, and all the other duplicates are just dropped. To enable

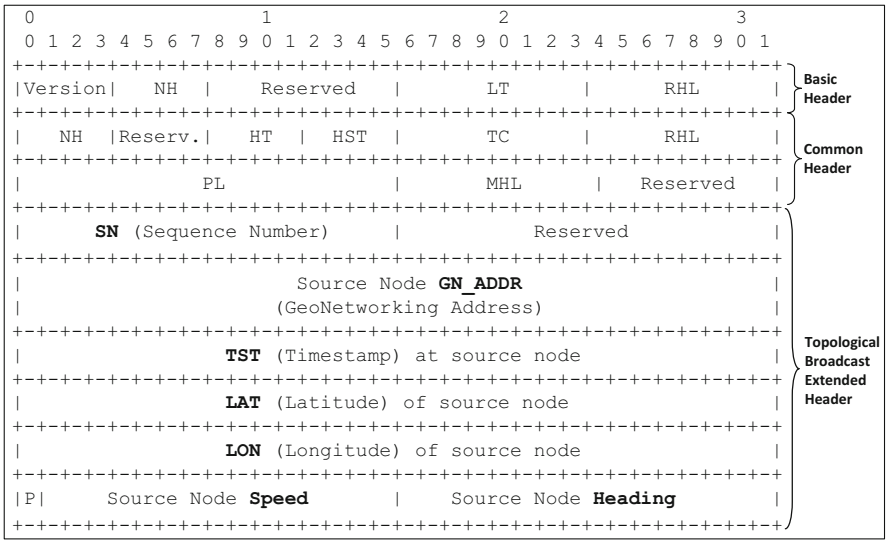

Fig. 8.13 Packet structure and headers of the GeoNetworking Topological Broadcast packet

such a duplicate packet detection mechanism, a Sequence Number (SN) has been added to the extended header of the Topological Broadcast packet, as well as in the other forwarding broadcast protocols (e.g., GeoBroadcast, etc.). See Sect. 8.7 for more details.

Differently from SHB, in Topological Broadcast the fields RHL and MHL in the Basic and the Common headers, respectively, are set with the number of hops requested by the user.

When receiving a new Topological Broadcast packet, the receiver node decodes it and checks if a similar packet has not been already received and processed in the past. If the packet has not been processed before, the contained payload is extracted and passed to the upper layer. Then, the value in the RHL field is reduced by one. If the new value of the RHL in the basic header is greater than one, the packet is rebroadcasted.

8.5.3.3 Example of Usage

Figure 8.14 shows an example of a vehicle using topological broadcast communication to search for a wanted service or information within the surrounding environment. A request for the specific service or information is then disseminated to not only those nodes within the communication range, but also to far-away neighbors through multi-hop forwarding. Any node (vehicle or road-side unit) that provides the requested service or information, can reply to the requester through a defined communication mechanism.

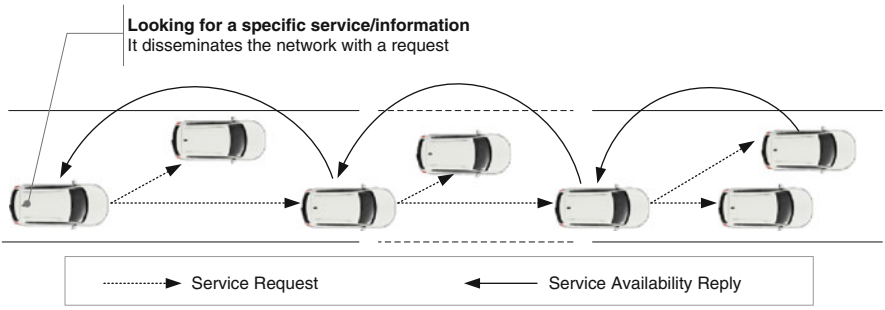

Fig. 8.14 A vehicle disseminates the network with a service request through a topological-broadcast communication to search for any node that can provide the desired service/information

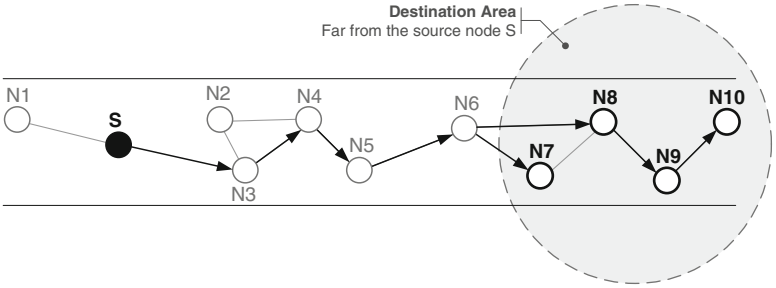

Fig. 8.15 GeoBroadcast communication scenario—sender outside the destination area

8.5.4 GeoBroadcast/GeoAnycast

GeoBroadcast and GeoAnycast protocols are very similar, especially from the view point of the data structure.This is the main reason why they are presented here under the same section. For the same reason, in other materials such as [4] the two protocols are presented together. Both protocols target a geographical area as destination. In GeoBroadcast the transmitted information is intended for all nodes located within the destination area, while in GeoAnycast the target is only the first node located within the destination area.

8.5.4.1 Scenario

GeoBroadcast intends to distribute information to a geographical area. Depending if the sender is inside the destination area or not, two types of GeoBroadcast scenarios can be identified as shown in Figs. 8.15 and 8.16. In Fig. 8.15 the sender is outside of and away from the dissemination area. In such a scenario, the GeoBroadcast packet first has to reach the destination area via a line forwarding (i.e., GeoUnicast fashion) and, once inside the destination area the packet is broadcasted to all nodes.

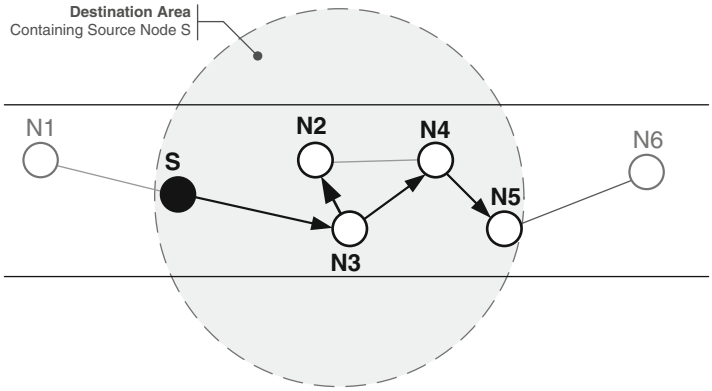

Fig. 8.16 GeoBroadcast communication scenario—sender inside the destination area

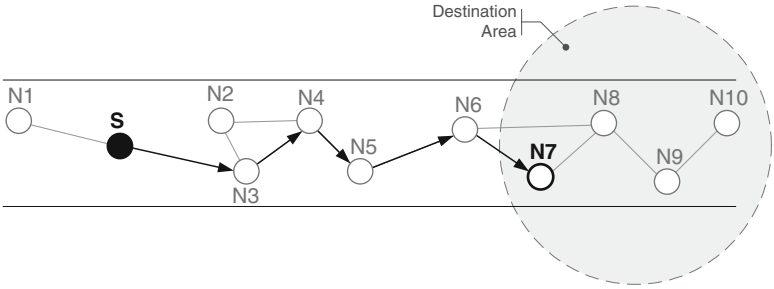

Fig. 8.17 GeoAnycast communication scenario

In Fig. 8.16, the sender is already inside the destination area, and the GeoBroadcast is immediately broadcasted to all nodes.

GeoAnycast can be looked at as a sub-set of GeoBroadcast, as the packet is always forwarded towards a geographical area. While GeoBroadcast targets all nodes within the destination area, the GeoAnycast target only one node within the destination area. Figure 8.17 shows a GeoAnycast communication scenario, where the packet is line forwarded till it reaches a first node inside the destination area (so far similar to GeoBroadcast), and then stops at that first node as it is considered as the destination node. In the case of GeoBroadcast, it would not have stopped at this node, but broadcasted to all other nodes within the destination area.

8.5.4.2 Protocol Operations

Whenever a node receives a payload from upper layer to disseminate to any node or all nodes within a specific geographical area, a GeoNetworking GeoBroadcast/GeoAnycast communication scheme is triggered and a GeoBroadcast/GeoAnycast packet is created (as shown in Fig. 8.18). The HST field in the

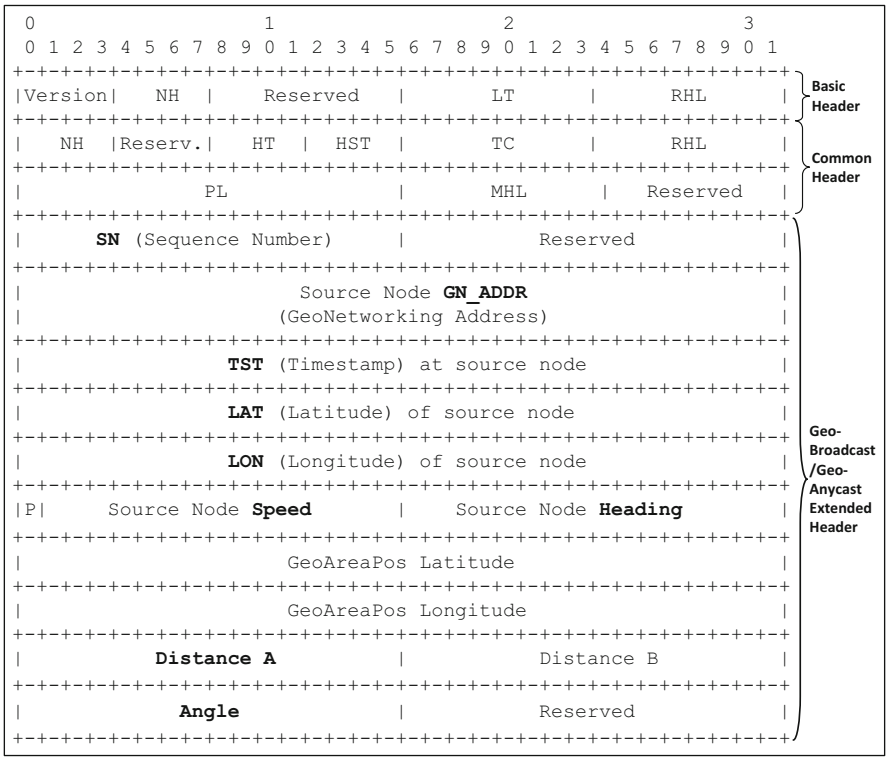

Fig. 8.18 Packet structure and headers of the GeoNetworking GeoBroadcast and GeoAnycast packets

common header is filled in a way to reflect whether the destination is any node (GeoAnycast) or all nodes (GeoBroadcast) in the destination area. The Extended header is composed of two parts, a first part dedicated to carry the information (GN_ADDR, timestamps, and location) of the sender (source node), and a second part is dedicated to carry the information of the destination area. Once the packet is prepared and filled in, the sender checks whether it is inside the destination area or not. If the sender is inside the destination area, the packet is broadcasted to all nodes around, otherwise the packet is line forwarded towards the destination area (i.e., towards the geographical point represented by GeoAreaPos Latitude and GeoAreaPos Logitude information in the extended header).

If a forwarder node receives a new GeoBroadcast or a new GeoAnycast packet intended for a destination area which does not surround that receiver node, and this packet has been received from a sender node which does not belong to the destination area either, then it forwards the packet to continue the line forwarding towards the destination. In case the packet has been received from a sender node which is located inside the destination area, that packet is ignored and dropped immediately.

If a node receives a GeoBroadcast or a GeoAnycast packet for which it is within the intended destination area, the packet is consumed immediately (decoded and payload moved up to upper layer). If the received packet is a GeoBroadcast packet, and the received node has been selected for forwarding the packet, then the packet is re-broadcasted to all nodes around to continue the dissemination of the packet within the destination area.

A GeoNetworking packet might be buffered for a defined duration of time due to the unavailability of the forwarding resources or for other reasons as explained in Sect. 8.4.

8.5.4.3 Example of Usage

Figure 8.19 shows an example to help understanding the usage of line forwarding and GeoBroadcast mechanisms, which are the key features in both GeoBroadcast and GeoAnycast protocols. In the example an emergency vehicle wants to inform all relevant vehicles located around the next road intersection about its arrival to allow a smooth and safe intersection crossing. The information about the approaching emergency vehicle is disseminated to all nodes within the destination area, including both vehicles and traffic lights. As the destination area is far-away, the packet is first line-forwarded through intermediate forwarders till it reaches a vehicle or any communicating node inside the targeted area, then broadcast within that area.

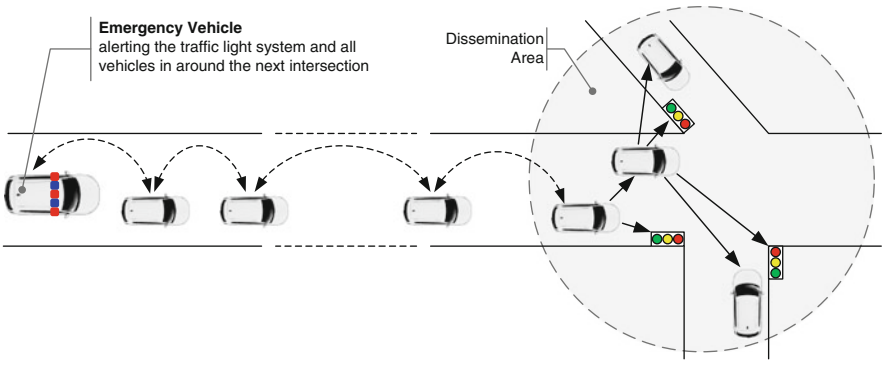

Fig. 8.19 Approaching emergency vehicle use-case enabled by dissemination of Decentralized Environmental Notification Message (DENM) (See Chap. 5 for more details about DEN Messages.) through GeoNetworking GeoBroadcast communications

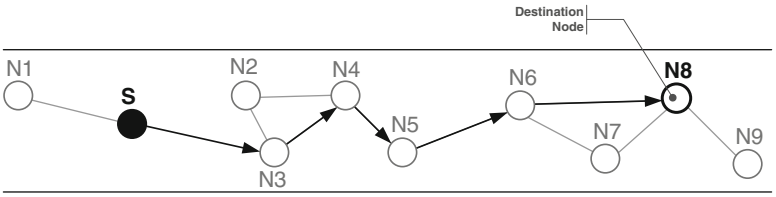

Fig. 8.20 GeoUnicast (Peer-to-Peer) communication scenario

8.5.5 GeoUnicast

GeoUnicast is usually intended for disseminating non-critical safety applications, as the number of beneficiaries is limited to two peers: the sender and the receiver. GeoUnicast is used to transmit a packet from one node (sender node) to another node (destination node) either through a direct communication link (One hop) if the two peers are within the communication range, or through multiple forwarding steps utilizing intermediate nodes.

8.5.5.1 Scenario

Figure 8.20 presents the GeoUnicast scenario through a peer-to-peer communication example. In the shown example, a node S initiates a peer-to-peer communication with a node N8 which is located beyond its communication range. A GeoUnicast packet is transmitted by the source node S, then forwarded by a selected neighbor N3, then N4 and so on till it reaches the destination node N8 through N6.

8.5.5.2 Protocol Operations

Whenever a node receives a payload from upper layer to transmit to a specific GeoNetworking node, a GeoNetworking GeoUnicast communication scheme is triggered and a GeoUnicast packet is created (as shown in Fig. 8.21). The GeoUnicast extended header is composed of two parts: a first part dedicated to carry the information (GN_ADDR, timestamps, and location) of the sender (source node), and a second part is dedicated to carry the information of the destination node. The upper layer provides the GeoNetworking address (GN_ADDR) of the destination node, without its location. Therefore, the source node first checks locally in its location table if there is any fresh entry that can provide the location of the destination. If the location of the destination node is missing, then a special mechanism (Location Service) as described in Sect. 8.5.5.3 is triggered to recover it. Such mechanism is necessary because the GeoUnicast packet can be transmitted only is the location information of the destination node is known.

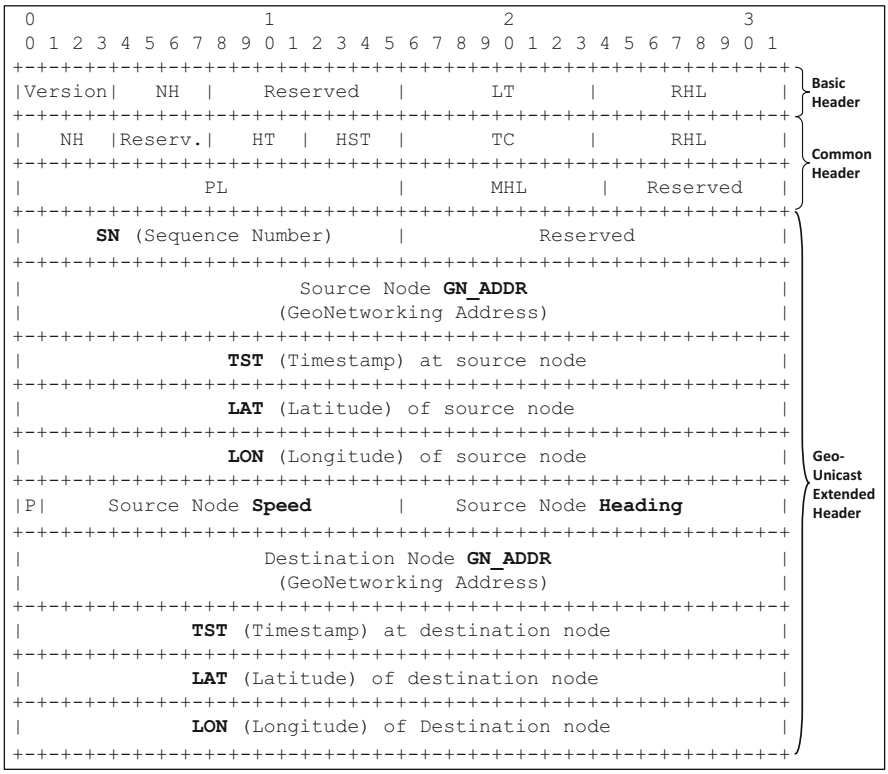

Fig. 8.21 Packet structure and headers of the GeoNetworking GeoUnicast packet

Once the GeoUnicast packet is prepared and filled in with all required information, it is transmitted either in broadcast mode or unicast mode depending on either sender-based or receiver-based forwarding mechanism is used (see Sect. 8.4 for more details). If sender-based forwarding is used, then the source node has to select the best forwarder among all its neighbors and then transmit the packet to that selected node through a unicast transmission. If a receiver-based forwarding mechanism is used, then the source node does not care about the selection of the next forwarder, and immediately broadcast the packet. Such packet is received by all neighbors, which enter in sort of competition to elect the next forwarder. When receiving a new GeoUnicast packet, a forwarder node has to check if the packet is not intended to itself (i.e., if it is not the destination). If it is the case, the packet is consumed immediately, otherwise the forwarding mechanism continues through selected neighbors, i.e. next forwarders.

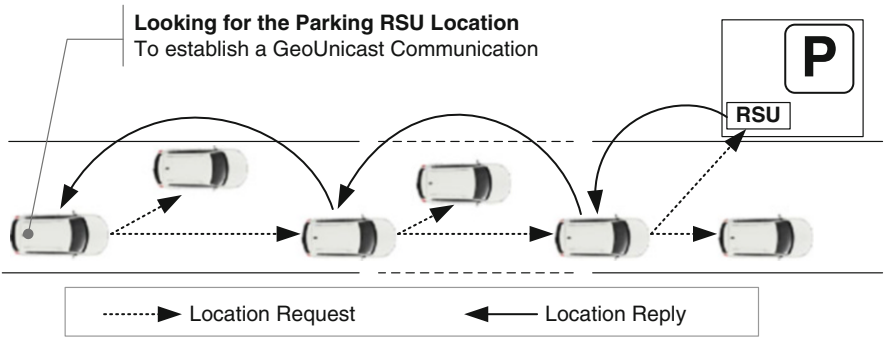

Fig. 8.22 Location Service Request and Reply packets exchange to recover the location of GeoUnicast destination node

8.5.5.3 Location Service

It might happen that the local location table does not contain fresh location information of the destination node. In such a case, the GeoUnicast cannot be performed. To overcome this, a location service is used to recover the location information of the destination node. Such a service is simple and basic, where the sender floods the network (surrounding nodes) with a Location Request packet by means similar to the Topological Broadcast scheme. Whenever it reaches either the requested node (i.e., the destination node of the GeoUnicast communication), or any other node in the network which has up-to-date information about the location of the destination node, a Location Reply is immediately transmitted towards the Source node (i.e., the node which initiated the GeoUnicast communication) using a mechanism similar to GeoUnicast forwarding. Figure 8.22 shows a typical example of Location Request and Reply packets exchange.

Once the Location Request packet reaches the requesting node with fresh information about the location of the designated destination node, all the GeoUnicast packets that have been buffered and that are destined to that particular destination node are extracted, updated (filling the destination node information in the GeoUnicast extended header), and then transmitted.

8.5.5.4 Example of Usage

Figure 8.23 shows a peer-to-peer communication based on GeoNetworking GeoUnicast exchange of packets between a vehicle and a parking lot. In the shown example, a vehicle sends a GeoUnicast packet which contains a request for parking reservation. The parking RSU replies with a GeoUnicast packet to confirm the parking availability along with a reservation number.

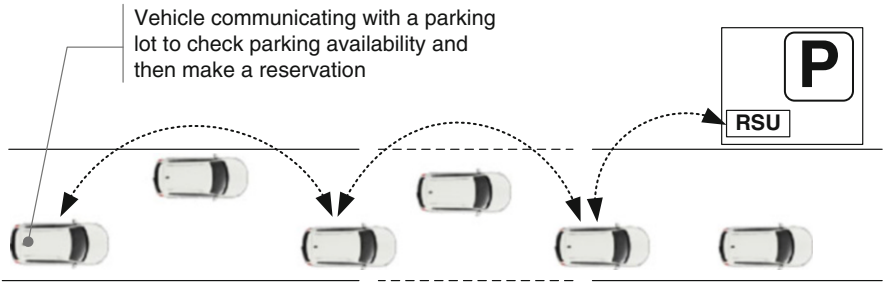

Fig. 8.23 GeoUnicast communication between a vehicle and a parking RSU to check parking availability and make a reservation

8.6 Security

This section is intended to give a brief overview on how security, as part of the ITS Station reference architecture, is integrated into GeoNetworking. For more details on security in VANETs, see Chap. 10.

The GeoNetworking layer may use the Security entity of the local node to provide secure communication services. This includes signing of messages and signature validation as well as end-to-end encryption. The selection of the mechanisms for a packet is based on a security profile supplied by the application or facility layer.

Security can be enabled via the `itsGnSecurity` protocol option. In secure mode GeoNetworking uses the following security services:

- **SN-ENCAP** is used to encapsulate each packet generated by the local node in a security envelope. Depending on the security profile, packets are signed, encrypted or both. The security entity also manages the inclusion of certificates on a regular basis or on demand.
- **SN-DECAP** is used to decapsulate a secured packet and remove the security envelope. Depending on the received packet this process includes verification of the signature, decryption of the packet or both. The result of the decapsulation and the packet without the security envelope are returned back to GeoNetworking for further processing.
- **SN-IDCHANGE-SUBSCRIBE**, **SN-IDCHANGE-UNSUBSCRIBE**, and **SN-IDCHANGE-EVENT** are used by GeoNetworking to be notified about changes of the node's pseudonym. Since some parts of the local GeoNetworking address are derived from the pseudonym the address is also updated with each pseudonym change.

Figure 8.24 illustrates the basic flow of protocol operation for an outgoing packet. First, all headers (basic, common and the packet type specific extended header) are created. In case security is enabled, the packet is handed to the Security

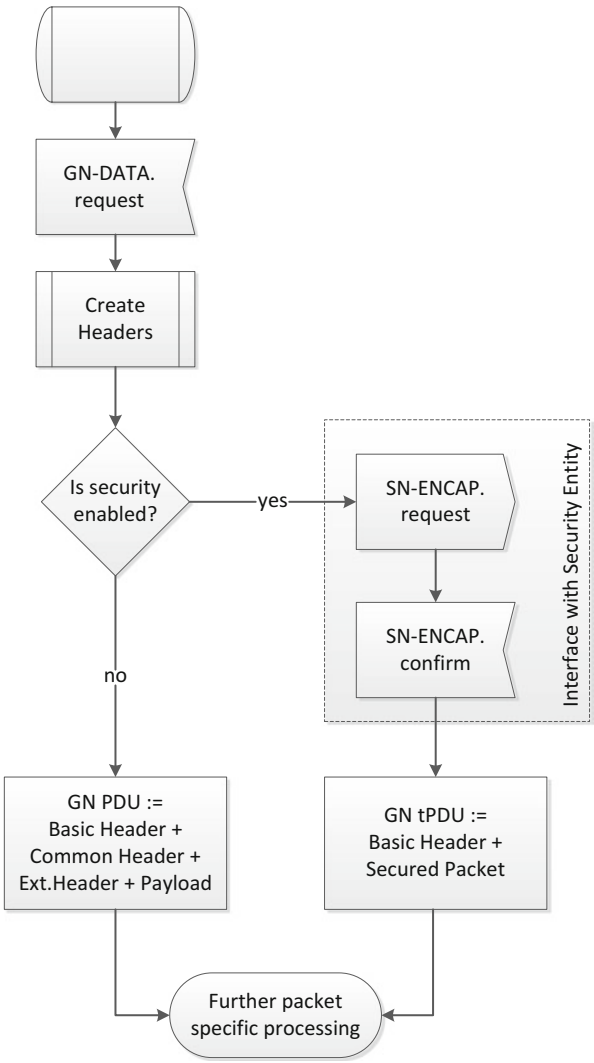

Fig. 8.24 Protocol operation for outgoing packets

Entity (SN-ENCAP.request). A *Secured Packet* is returned (SN-ENCAP.confirm) that contains all the information from the common and extended header as well as the packet payload in a signed and/or encrypted format. The specific security operations applied to create the Secured Packet are defined by the *Security Profile* provided with the encapsulation request. The Secured Packet is appended to the basic header to create the GeoNetworking PDU.

Figure 8.25 shows the protocol operation for an incoming packet. First the basic header is processed. If the field for the next header indicates a Secured Packet, the data following the basic header is handed to the Security Entity for decapsulation (SN-DECAP.request). The result (SN-DECAP.confirm) consists of a decapsulation

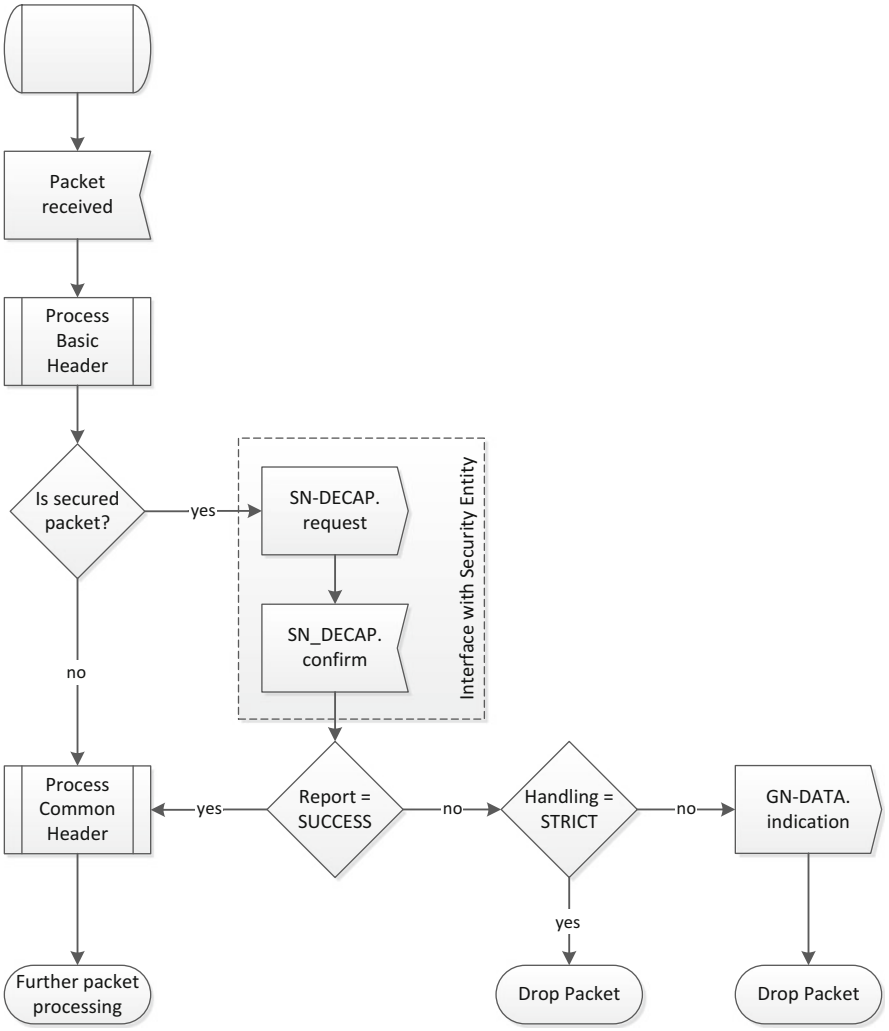

Fig. 8.25 Protocol operation for incoming packets

report, the plain packet data, and additional security related parameters. If the report indicates a success, the remaining headers and payload are processed similar to unsecured packets. In case of a failed security check packets are dropped without further processing. However, the GeoNetworking standard [4] provides a *non-strict* operation mode in which the payload of packets with failed verification is still handed to upper layers to allow for additional security evaluation on facility or application levels. Nevertheless, secured packets are only forwarded if the security check was successful.

8.7 Duplicate Packet Detection

GeoNetworking protocol is built around the concept of maximizing the spreading of information in a geographical area and for this reason each packet might be retransmitted several times within an area. For example, in the case of GeoBroadcast, each receiving host will retransmit the packet if either the hop count is greater than zero or the host is inside a defined geographical area. But, similar behavior might happen in case of routing loops, misconfiguration or replay of packets from misbehaving nodes.

For this reason, in order to control (e.g., prevent) the forwarding of duplicate packets, the GeoNetworking protocol uses mechanisms for duplicate packet detection:

- **Sequence number and time stamp-based:** This technique, applicable for Topological Broadcast, Geobroadcast, GeoAnycast, and GeoUnicast protocol operations (see Sects. 8.5.3–8.5.5), makes use of both sequence number and time stamp included in the transmitted packet to evaluate if a packet is duplicated or not.
- **Time stamp-based:** This technique makes use only of the time stamp and it is suitable for SHB protocol operation (see Sect. 8.5.2).

It is important to remind that GeoNetworking is able to detect packet duplication, however it does not provide any packet re-ordering and due to the simple duplicate packet detection, out-of-sequence packets are discarded.

8.8 Special Features

In order to provide differentiated and reliable support to vehicular applications, GeoNetworking contains special features which address Quality of Service (QoS):

- Traffic Classes
- Packet Data Rate Control
- Decentralized Congestion Control

In the case of *Decentralized Congestion Control*, the functionality might be applicable only to a particular media (e.g., ETSI ITS-G5). The other special features are instead available for any media on top of which GeoNetworking is relying.

8.8.1 Traffic Classes

QoS is especially important for safety where different applications should have a corresponding priority level. For example, a safety service should have a higher priority than a service for advertisements. For this reason, GeoNetworking uses classes to prioritize the network traffic. Each packet contains a dedicated field *Traffic Class* (TC) which contains the following information:

- **SCF** indicates whether the packet shall be buffered when no neighbor exists.
- **Channel Offload**[3] indicates whether the packet can be offloaded to another channel than specified in the TC ID.
- **TC ID** identifies which traffic class should be used.

SCF and *Channel Offload* are used within GeoNetworking to perform forwarding operations. In particular, the former is used by GeoNetworking to decide what to do once a packet should be transmitted but the location table is empty. Figure 8.26 provides an example of how GeoNetworking behaves depending on SCF value as provided by the upper layer. The latter allows (or not) GeoNetworking to transmit a packet on a different TC from the one specified inside the packet. With ETSI ITS-G5 the *TC ID* is used to decide which 802.11e [9] queue shall be used.

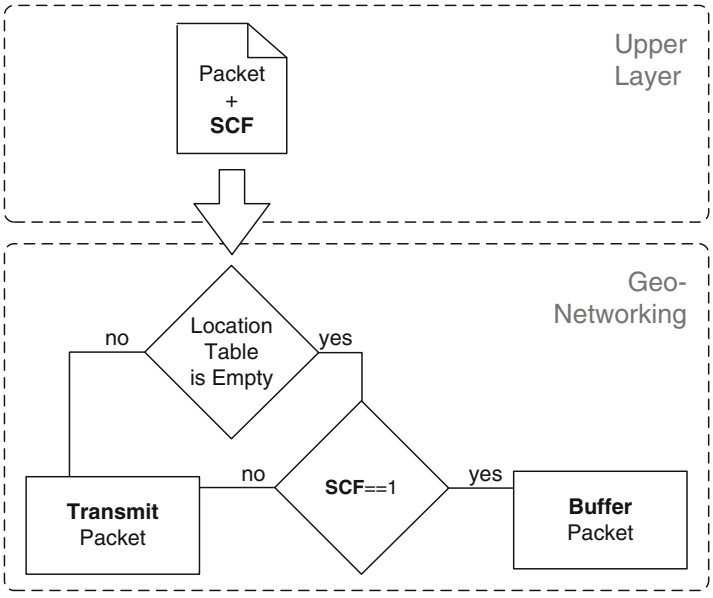

Fig. 8.26 Example of GeoNetworking behavior depending on SCF

[3] See Chap. 6 for more details about offloading between channels.

8.8.2 Packet Data Rate Control

Forwarding a packet is one of the main functionalities of GeoNetworking. But, in the case a misbehaving node is generating too many packets the network could be easily flooded locally and damages could be potentially created far away from the originator due to forwarding.

GeoNetworking addresses this problem by providing a *Packet data rate control* functionality which is evaluating the quantity of generated packets by each neighbor and limiting the forwarding of packets from a misbehaving node. In order to realize this, each node maintains an Exponential Moving Average (EMA) of the Packet Data Rate (PDR) for each entry in the location table. The calculation of the EMA is available in Eq. (8.1):

$$\text{PDR} = \beta \times \text{PDR}_{t-1} + (1 - \beta) \times x_t \tag{8.1}$$

where:

x_t is the measured instantaneous value of the packet data rate upon reception of the GeoNetworking packet.
PDR is the average value of the packet data rate at time t;
PDR_{t-1} is the previous value at time $t - 1$ maintained in the location table.
β is the weighting factor ($0 < \beta < 1$)

In the case the EMA is above a predefined threshold, the packets of the particular node are not forwarded.

8.8.3 Decentralized Congestion Control at Network Layer

In case safety vehicular applications run on top of IEEE 802.11p, the so-called DCC [2][4] feature is required. In fact, it is well known that the CSMA/CA mechanism used by IEEE 802.11p provides a fair channel access to the contending nodes, i.e., on average, it lets nodes access the channel the same number of times in a given time period. However, in the short run, it is inherently unpredictable and due to the random exponential back-off procedure the interference between concurrent transmissions may lead to transmission failures. DCC makes use of the local knowledge about the channel status to adjust the transmission parameters and thus reducing channel congestion.

GeoNetworking extends this concept by providing the capabilities of disseminating the information about the Channel Busy Ratio (CBR) measured locally to surrounding nodes. By disseminating CBR values, the neighbors increase their awareness of possible channel congestion that the ego node can contribute to, even

[4] See Chap. 7 for more details about DCC.

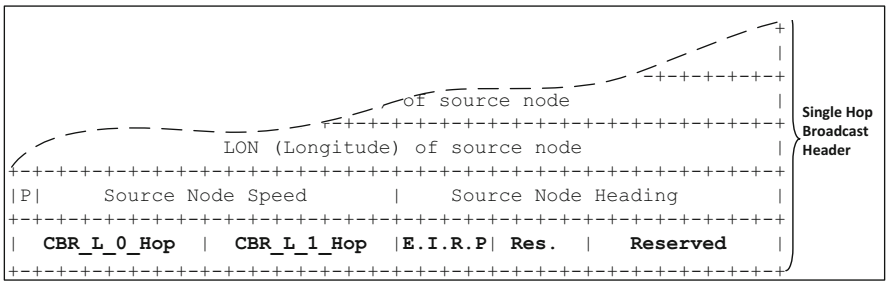

Fig. 8.27 DCC fields included in the SHB packet

though the ego node does not perceive a local congested channel status. In general the dissemination of CBR values allows to react quickly to congestion and maintains globally fair the usage of the channel. More information could be found in [12].

GeoNetworking supports the transmission of CBR values directly in the header of every transmitted SHB packet. Figure 8.27 shows the DCC related fields which are included in the SHB packet:

- CBR_L_0_Hop represent the CBR value based on neighbor information,
- CBR_L_1_Hop represent the maximum CBR_L_0_Hop value received from a neighboring node in a given interval,
- output power of the current packet—EIRP,
- reserved for future Multi Channel Operations.

8.9 Conclusion

In this chapter the base of routing has been discussed, the differences between multiple addressing techniques used in GeoNetworking have been identified and the principles in the position-based forwarding have been clarified. Such features are the core techniques on top of which Geonetworking functionalities are built. Such functionalities have been standardized in ETSI TC ITS as a multi-series standards [4, 5] which is going to be used in Europe for the initial deployment of vehicular communication. Multiple examples of the usage of Geonetworking have been provided in the chapter to simplify the comprehension of this technology for both technical and non-technical readers.

References

1. ETSI EN 302 665 (V1.1.1): Intelligent transport systems (ITS); communications architecture (2010)
2. ETSI TS 102 687 (V1.1.1): Intelligent transport systems (ITS); decentralized congestion control mechanisms for intelligent transport systems operating in the 5 GHz ranger; access layer part (2011)

3. ETSI EN 302 636-1 (V. 1.2.1): Intelligent transport systems (ITS); vehicular communications; GeoNetworking; Part 1: Requirements (2013)
4. ETSI EN 302 636-4-1 (V1.2.0): 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 (2013)
5. ETSI TS 102 636-4-2 (V 1.1.1): Intelligent transport systems (ITS); vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5 (2013)
6. ETSI EN 302 636-3 (V1.1.2): Intelligent transport systems (ITS); vehicular communications; GeoNetworking; Part 3: Network architecture (2014)
7. ETSI TS 102 894-2 (V1.2.1): Intelligent transport systems (ITS); users and applications requirements; Part 2: Applications and facilities layer common data dictionary (2014)
8. Füßler H, Widmer J, Käsemann M, Mauve M, Hartenstein H (2003) Contention-based forwarding for mobile ad-hoc networks. Elsevier's Ad Hoc Netw 1(4):351–369
9. IEEE Computer Society. IEEE Std 802.11eT, Part 11: Wireless medium access control (MAC) and physical layer (PHY) specifications: medium access control (MAC) enhancements for quality of service (2005)
10. Karp B, Kung HT (2000) GPSR: greedy perimeter stateless routing for wireless networks. In: Proceedings of the 6th annual international conference on mobile computing and networking, MobiCom '00. ACM, New York, pp 243–254
11. Mariyasagayam M, Osafune T, Lenardi M (2007) Enhanced multi-hop vehicular broadcast (mhvb) for active safety applications. In: IEEE 7th international conference telecommunications, ITST'07, pp 1–6
12. Tielert T, Jiang D, Chen Q, Delgrossi L, Hartenstein H, (2011) Design methodology and evaluation of rate adaptation based congestion control for vehicle safety communications. In: IEEE vehicular networking conference (VNC), pp 116–123. doi:10.1109/VNC.2011.6117132