Chapter 2

Literature Review

The chapter explores the initial developments that were carried out in creating a broadcast protocol. During the last few years, a lot of broadcasting protocols for VANETs have been reported in literature. They can be generally classified into two main categories according to the spreading of information packets in the network. These categories are (Li and Wang Willke, Tientrakool, and Maxemchuk Panichpapiboon and Pattara-atikom Festag, Papadimitratos, and Tielert Hall) Junhai et al. Badarneh and Kadoch Sebastian et al. Lua et al. Zhou et al. Shevade et al. Guo, Ammar, and Zegura Chu and Huang) as follows:

• Single-hop Broadcasting: In Single-hop Broadcasting, information packets are not flooded by vehicles. Instead, when a message is received by a vehicle, information is kept in the vehicle’s On-Board database. Periodically, every vehicle selects some of the records stored in its database to broadcast. Hence, in Single-hop Broadcasting, each vehicle carries the traffic information with it as it travels, and this information is transferred to all other vehicles in its one-hop neighborhood in the next broadcast cycles. Ultimately, vehicle’s mobility is involved in spreading the information in Single-hop Broadcasting protocol.

• Multi-hop Broadcasting: In Multi-hop Broadcasting strategy, a message is spread in a network through flooding. In general, when a sender vehicle broadcasts an information message, a number of vehicles within the vicinity of the sender will become the next relay vehicles, by rebroadcasting the message fur-
2.1 Single-hop Broadcasting Protocols

In Single-hop Broadcasting, vehicle periodically disseminates some of the information in its database to the other vehicles in the network. Broadcast interval and information are the two choices that need to be considered while designing the broadcast protocol for VANETs. To keep the most up-to-date information without redundancy, the broadcast interval must be set appropriately. It should neither be too long nor too short. Apart from this, important and relevant information should only be selected to broadcast. Single-hop Broadcasting protocols can be further divided into following two categories:

a. Fixed Interval Based Single-hop Broadcasting Protocols


2.1.1 Fixed Interval Based Single-hop Broadcasting Protocols

Fixed broadcast interval protocols focuses only on the selection and aggregation of information. TrafficInfo (Zhong, Xu, and Wolfson) is an example of fixed broadcast interval protocol in which every vehicle is equipped with a Global Positioning System (GPS) and digital road map and periodically broadcasts the traffic information stored in its database. A particular type of traffic information reported during the travel times on the road segments. During broadcasting process, each vehicle stores its own travel time and time taken by other vehicles during travelling into the database. Although Single-hop Broadcasting scheme is inefficient in broadcasting all the records from database, TrafficInfo uses the bandwidth efficiently and broadcasts only the most relevant information from the database. The relevance of the information is determined by a ranking algorithm, which is based on the current location of the vehicle and the current time.
TrafficView is another single-hop fixed interval broadcasting scheme (Nadeem et al.) designed for enabling an exchange of traffic information among vehicles. Speed and position are two information types that are exchanged among vehicles. In this scheme, when a vehicle receives a broadcasted message, it first stores the information in its database. The information is then rebroadcasts in the next broadcast cycle. However, instead of broadcasting all stored record from the database, only a single record is broadcasted after aggregating the multiple records. Ratio-based and the cost-based are the two algorithms that are used for aggregation. In the ratio-based algorithm, a road is divided into smaller regions, and an aggregation ratio is assigned to each region according to the importance of the region and the level of accuracy required for that region. In cost-based algorithm, cost can be regarded as the loss of accuracy incurred from combining the records. Simulation shows that although the cost-based algorithm yields better accuracy, the ratio-based algorithm gives more flexibility.

2.1.2 Adaptive Interval Based Single-hop Broadcasting Protocols

In adaptive broadcast interval protocols, an adjustment of broadcast intervals is also taken into consideration. Collision Ratio Control Protocol (CRCP) (Fujiki et al.) uses adaptive broadcast interval in which each vehicle disseminates the traffic information periodically. The traffic information in this case is the location, speed and road ID. This information is measured every second. This protocol employs a mechanism for dynamically changing the broadcast interval based on the number of message collisions. Basically, the protocol aims at keeping the collision ratio at a targeted level regardless of the vehicle density. Intuitively, the number of message collisions increases with an increase in network density. Apart from adaptive broadcast interval mechanism, three methods Random Selection (RS), Vicinity Priority Selection (VPS), and Vicinity Priority Selection with Queries (VPSQ) are proposed for selecting the data to be disseminated.

Abiding Geo-cast protocol (Yu and Heijenk) is another example of adaptive broadcast interval protocol which was designed to disseminate safety messages within a useful area where these messages are still relevant. In this scheme, a vehicle which
detects an emergency situation first starts broadcasting a warning message. Message specifies the area where the warning is still relevant. When another vehicle receives the warning message, it will act as a relay node and keep broadcasting the warning message as long as it is still traveling in the concerned area. Each vehicle adjusts its rebroadcast interval dynamically in order to reduce the number of redundant warning packets. The rebroadcast interval is decided by the transmission range, speed and the relative distance between the emergency site and the vehicle.

Segment-oriented Data Abstraction and Dissemination (SODAD) protocol (Wischhof, Ebner, and Rohling) also uses adaptive broadcast interval in which roads are divided into segments of predefined length. Each vehicle collects the data by sensing the information itself and from the reports of other vehicles. Each vehicle adaptively adjusts its broadcast interval to reduce the redundancy.

Information received from other vehicles is characterized in two ways:

- Provocation
- Mollification

A provocation event, is an event that reduces the time until next broadcast, whereas a mollification event, is defined as an event that increases the time until next broadcast. When a vehicle receives a message, it determines whether it is a provocation or a mollification event by assigning a weight, to the received message. Weight is calculated from the discrepancy between the received data and data available in vehicles knowledge database. The weight will be high if the received information is newer than the stored information. Based on the message weight, node determines whether a provocation or mollification event has occurred by comparing it with a threshold. The time for next rebroadcast is increased or decreased depending on the weight.

2.2 Multi-hop Broadcasting Protocols

In Multi-hop Broadcasting (Korkmaz, Ekici, and Uner, Fasolo, Zanella, and Zorzi, Li et al., “A Distance-Based Directional Broadcast Protocol for Urban Vehicular ad-hoc Network” Wisitpongphan et al., Taha and Hasan, Schwartz et al.), flooding is used for message propagation in the network. However, a pure flooding is inefficient because, it lacks scalability and message collision. Redundancy increases as the network becomes
denser and reduces throughput, thereby reducing network scalability. In addition, message collision is another critical problem because multiple vehicles in the same region may rebroadcast the message at the same time. This is called broadcast storm problem \cite{Ni et al.}. Multi-hop broadcasting can further be divided into the following three categories \cite{Bilal, Chan, Pillai, Alshaer and it Wegener et al., Katti et al., Li et al., Yang and Wu, Kadi and Agha, Qayyum, Viennot, and Laouiti}:

\begin{enumerate}
\item [a.] Delay Based Multi-hop Broadcasting Protocols
\item [b.] Probability Based Multi-hop Broadcasting Protocols
\item [c.] Network Coding Based Multi-hop Broadcasting Protocols
\end{enumerate}

### 2.2.1 Delay Based Multi-hop Broadcasting Protocols

In a Delay Based Multi-hop Broadcasting scheme, different waiting time before rebroadcasting the message is assigned to each receiving vehicle. Fundamentally, the vehicle having the shortest waiting time gets the highest priority to rebroadcast the message. In addition, redundancy is avoided by other vehicles by aborting their waiting process once they know that the message has already been rebroadcasted. While different delays are assigned to each vehicle in delay-based broadcasting protocols, a different rebroadcast probability is assigned to each vehicle in a probabilistic protocol.

Urban Multi-hop Broadcast (UMB) protocol \cite{Korkmaz, Ekici, and Uner} is a delay based multi-hop broadcasting protocol designed to solve the broadcast storm, the hidden terminal, and the reliability problems in multi-hop broadcasting. UMB divides a road within the transmission range of a transmitter vehicle into smaller segments, and it gives the rebroadcast priority to the vehicles that belong to the farthest segment.

UMB uses two types of message forwarding:

\begin{enumerate}
\item [a.] Directional Broadcast
\item [b.] Intersection Broadcast
\end{enumerate}
UMB is inefficient because, next rebroadcast vehicle has to wait for the longest time before being able to transmit the Clear-To-Broadcast (CTB) message. This is due to the longest black-burst duration is assigned to the next rebroadcast vehicle.

Smart Broadcast (SB) \cite{Fasolo, Zanella, and Zorzi} was proposed to improve the shortcomings of UMB protocol. In SB, when a source vehicle has a message to send, it transmits a Request-To-Broadcast (RTB) message containing its location and other information such as message propagation direction and contention window size. Also, all vehicles in the range of the source that receive the RTB message determine the sector in which they belong to, by comparing their locations with that of the source vehicle. Next, all vehicles that receive the RTB message choose a contention delay based on the sector that it resides.

Efficient Directional Broadcast (EDB) protocol \cite{Li et al., "A Distance-Based Directional Broadcast Protocol for Urban Vehicular ad-hoc Network"} is another delay-based multi-hop broadcast protocol that works somewhat similar to UMB and SB protocols. However, it does not use RTB and CTB control packets. EDB also exploits the use of directional antennas. In particular, it is proposed that each vehicle is equipped with two directional antennas, each with 30-degree beam width. Similar to UMB protocol, EDB also uses two types of message forwarding, namely directional broadcast on the road segment and directional broadcast at the intersection.

Slotted 1-Persistence Broadcasting protocol \cite{Wisitpongphan et al.} is a message forwarding approach, similar to those of the other delay-based multi-hop broadcasting protocols, in which the vehicles that are farther away from the transmitter will get the rebroadcast priority. In this protocol, when a vehicle receives a message, it rebroadcasts the message according to an assigned time slot, where the time slot is a function of distance between the vehicle and the transmitter. In particular, each vehicle computes the time slot in which it will rebroadcast the message based on the following equation 2.1:

\[
T_{S_{ij}} = S_{ij} \ast \tau
\]  

\hspace{1cm} (2.1)

where \( \tau \) is an estimated one-hop propagation and medium access delay, and \( S_{ij} \) is the assigned slot number.
Reliable Broadcasting of Life Safety Messages (RBLSM) (Taha and Hasan) is also a class of delay based multi-hop broadcasting, in which, as soon as a node receives a message from source, it determines the waiting time for rebroadcasting the message. In RBLSM, the priority is given to the vehicle nearest to the transmitter. The reason behind choosing the nearest vehicle as the next rebroadcast vehicle is that, it is considered to be more reliable than the other vehicles that are far away or at a distance from the transmitter. It is assumed that the nearer vehicle has better received signal strength. This protocol also uses the concept of RTB and CTB control packets. Performance evaluation is done via simulation with only single hop latency. Link-based Distributed Multi-hop Broadcast, (LDMB) is a similar protocol which assigns the waiting delay based on the link quality as proposed in (Schwartz et al.).

Fastest-Vehicle (Bilal, Chan, and Pillai), is another multi-hop routing protocol. It uses speed information of each vehicle for message transfer and distance of the selected vehicle from the destination vehicle. On the basis of speed v of the vehicles and distance s of the vehicles from the destination, the time t for each vehicle within the transmission range is calculated. The vehicle with the least time is selected as the next hop for data dissemination.

2.2.2 Probability Based Multi-hop Broadcasting Protocols

In probabilistic broadcasting approach, each vehicle rebroadcasts a message according to the assigned probability. Since, only few vehicles will rebroadcast the message, redundancy and message collisions are reduced. The third category of multi-hop broadcasting is network coding, which has caught attention in the field of ad-hoc wireless communications.

Weighted p-Persistence protocol (Wisitpongphan et al.) is a probability based broadcasting scheme, in which, a vehicle that receives a message for the first time computes its own rebroadcasting probability based on its distance from the transmitter. The distance can be computed by comparing its current position with the position of the transmitter specified in the message. In particular, the rebroadcast probability is computed from the following equation 2.2:

\[ P_{ij} = \frac{D_{ij}}{R} \] (2.2)
where $P_{ij}$ represents the probability between transmitter $i$ and vehicle $j$, $D_{ij}$ represents the distance between transmitter $i$ and vehicle $j$, and $R$ is the transmission range of transmitter $i$. On the basis of above equation, vehicles that are far away from the transmitter will get higher rebroadcast probabilities. However, vehicle density is not taken into consideration in this probability assignment function. Hence, in the dense network, the number of rebroadcast packets can still be large.

There is another protocol named, Optimized Adaptive Probabilistic Broadcast (OAPB) protocol (Alshaer and it), in which number of neighbors i.e. local vehicle density is also taken into consideration while determining the forwarding probability. Each vehicle exchanges HELLO packets periodically to select an appropriate forwarding probability. In particular, when a vehicle receives a message, it computes its own forwarding probability based on the following equation 2.3:

$$\bar{\phi} = \frac{P_1 + P_2 + P_3}{3}$$

(2.3)

where $P_1$, $P_2$, and $P_3$ are functions of the number of one-hop neighbors, the number of two-hop neighbors, and a set of two hop neighbors that can only be reached through a particular one hop neighbor (Alshaer and it).

Auto-Cast protocol (Wegener et al., “AutoCast: An Adaptive Data Dissemination Protocol for Traffic Information Systems”) is similar to OAPB in which the rebroadcast probability is determined from the number of neighbors around the vehicle. However, it uses a different probability function to obtain rebroadcast probability equation 2.4:

$$p = \frac{2}{N_h \times 0.4}$$

(2.4)

where $N_h$ is the number of one-hop neighbors. According to the above probability assignment function, the rebroadcast probability decreases as the number of neighbors increases. Evidently, this function can only work when the number of neighbors, $N_h \geq 5$. However, it is not clearly specified in [58] how the probability is assigned in the cases where $N_h < 5$. 
2.2.3 Network Coding Based Multi-hop Broadcasting Protocols

Network coding is a new way of information dissemination which can be applied to a deterministic broadcast approaches, resulting in significant reductions in the number of transmissions in the network and hence yields a much higher throughput than the traditional way of transmission.

COPE introduced in (Katti et al.) is based on the principle of network coding. Although COPE is a uni-cast routing protocol, it is a foundation for many multi-hop routing protocols. The COPE was intended to realize the benefits of network coding beyond the simple duplex flows.

The COPE was based on three key techniques:

a. Opportunistic listening,

b. Opportunistic coding, and


Opportunistic listening allows nodes to take the advantage of wireless broadcast medium by snooping all data packets. Each overheard message will be stored in the nodes buffer for a limited time period. These packets will later be used for network coding when the opportunity presents. Opportunistic coding, defines some basic rules for a node to encode and transmit a message. Basically, a node should ensure that its next hop neighbor has enough information to decode the encoded message that has been transmitted. Usually, a node will be able to correctly decode a message $i$ from an encoded message created from packets $p_1, p_2, ..., p_n$ if it has $n - 1$ of these packets. Thus, learning what packets its neighbors are having is crucial, and this is achieved with a periodic broadcast of reception reports. Hence, every node periodically announces packets that are stored in its reception buffer to all its neighbors.

CODEB is another network coding-based broadcasting protocol introduced in (Li et al., “Network Coding-based Broadcast in Mobile ad-hoc Networks”). It extends the concepts and techniques proposed in COPE to cover broadcasting scenarios in wireless ad-hoc networks. It uses opportunistic listening, where every node snoops all
packets overheard by it. In addition, each node periodically broadcasts the list of its one-hop neighbors. This allows all nodes to build a list of its two-hop neighbors, which will further be used to construct a broadcasting backbone. Moreover, CODEB relies on opportunistic coding, in which coding opportunities to transmit coded packets is determined. CODEB also pointed out that opportunistic coding for broadcast is somewhat different from coding for unicast. In broadcasting, all the neighbors of the node must receive the message where as in unicasting, only the intended next hop node receives a given message. Hence, broadcasting increases the level of complexity as all nodes that receive message must be able to decode.

Efficient Broadcasting Using Network Coding and Directional Antennas (EBCD) is a network coding-based broadcasting protocol which gains the benefit of both network coding and directional antennas [Yang and Wu]. EBCD similar to CODEB, determines a subset of neighboring nodes that can perform forwarding task deterministically. Although, Dynamic Directional Connected Dominating Set (DDCDS) algorithm is used by EBCD. As a result, a directional virtual network backbone is constructed by DDCDS, where each node determines both its forwarding status as well as the outgoing edges (antenna sectors) in which the packets can be transmitted. In EBCD, network coding is applied in each sector of the directional antennas around the node, whereas in CODEB, network coding applied is Omni-directional. EBCD shows significant improvement with directional antennas and network coding in terms of number of transmissions, compared to other schemes.

DifCode is also a network coding-based broadcasting protocol. Its goal was to reduce the number of transmissions required to flood packets in wireless ad-hoc network [Kadi and Agha]. Similar to CODEB, DifCode also chooses the next forwarding nodes deterministically. However, DifCode uses a selection algorithm based on multi-point relay (MPR) [Qayyum, Viennot, and Laouiti]. MPR of a node is the list of its one-hop neighbors that cover its two-hop neighborhood. In DifCode, nodes can encode and broadcast only those packets that are received from those nodes that select it as their MPR. DifCode and CODEB also differ by their opportunistic coding techniques. In CODEB, all neighbors of a transmitter decode the received packets immediately and hence limit coding opportunities. On the other hand DifCode relaxed this constraint by allowing nodes to buffer packets that are not immediately
2.3 CDS-BASED BROADCASTING

Decodable. Specifically, all nodes maintain buffers for keeping three different types of packets:

a. Successfully decoded packets,

b. Not immediately decodable packets, and

c. Packets that need to be encoded and broadcast further.

Simulation results show that DifCode results in lower redundancy rate than the probabilistic broadcasting protocols.

2.3 CDS-Based Broadcasting

The problem of designing efficient broadcast protocols for ad-hoc networks has been investigated for several years. Probably, the most common technique to reduce redundant transmissions in a broadcasting task is the use of connected dominating sets. Let $G(V,E)$ be the graph induced by the network topology, so that $V$ is the set of nodes in the network and $E$ represents the connectivity between them. Then, a subset $V_D \subseteq V$ is said to be dominating, if each node in $V$ either belongs to $V_D$ or has at least one neighbor which belongs to $V_D$. $V_D$ is Connected Dominating Set (CDS), if it is connected. In CDS-based broadcasting, only those nodes belonging to the Connected Dominating Set (CDS) are required to retransmit the broadcast message, and it will indeed reach the whole network. Therefore, fewer the number of nodes in the CDS, less redundant the broadcast protocol will be.

Unfortunately, the problem of finding the minimum CDS was shown to be NP-hard (Clark, Colbourn, and Johnson), and many heuristics have been proposed since then. (Wu and Li) described several lightweight backbone construction schemes. A modified definition from (Stojmenovic, Seddigh, and Zunic) and (Stojmenovic) of the basic concept in (Wu and Li), because of its reduced message overhead.

Assume that each node $x$ is identified by a unique key, $\text{key}(x)$. Then, a node is said to be an intermediate node if it has two unconnected neighbors (Wu and Li). A node $u$ is covered by neighboring node $v$ if each neighbor of $u$ is also a neighbor of $v$, and $\text{key}(u) < \text{key}(v)$. A node $u$ is covered by two connected neighboring nodes $v$ and $w$ if each neighbor of $u$ is also a neighbor of either $v$ or $w$ (or both), $\text{key}(u) < \text{key}(v)$,
and key(u) < key(w). An intermediate node not covered by any neighbor becomes an inter-gateway node. An inter-gateway node not covered by any pair of connected neighboring nodes becomes a gateway node. A set of gateway nodes form a CDS.

(Wu and Li) concepts require either one-hop knowledge of neighbors with their position, or two-hop neighbor topology information. Such information is obtained by exchange of periodic 'hello' (beacon) message exchange. Experimental data from several sources confirm that (Wu and Li) concepts provide small size CDS on average. Each node makes a decision about CDS membership without communication between the nodes, beyond the message exchange, node use decision to discover each other and establish neighborhood information.

A framework and general algorithm in (Stojmenovic, Seddigh, and Zunic) and (Stojmenovic) is based on two concepts:

- CDS as a particular type of backbone that provides reliability,
- Neighbor elimination scheme.

In NES (Stojmenovic, Seddigh, and Zunic), (Stojmenovic), (Peng and Lu), a node does not need to rebroadcast a message if, all its neighbors are believed to be covered by previous transmissions. After each received copy of the same message, a node eliminates, the neighbors that are assumed to have received the same message (based on local knowledge) from its rebroadcast list. If the list becomes empty before the node decides to rebroadcast, the retransmission is cancelled.

The general Dominating Set and Neighbor Elimination Scheme (DS-NES) (Stojmenovic, Seddigh, and Zunic), (Stojmenovic) for intelligent flooding proceeds as follows: the source node transmits the message. Nodes not in the CDS do not retransmit the message. Upon receiving the first copy of the message, a node in the CDS will select a time-out period to wait. It will also eliminate (originally containing all one-hop neighbors) all neighbors that received the same copy of the message from its forwarding list. While waiting, more copies of the message could be received. For each of them, all neighbors receiving it are eliminated from the forwarding list. When the time-out expires, the node will retransmit if its forwarding list is not empty, otherwise it will cancel retransmission. This framework was applied in (Stojmenovic, Seddigh,}
2.4 VANET-SPECIFIC BROADCASTING

and Zunic) and (Stojmenovic) using clustering-based and (Wu and Li) concept-based backbones.

The Parameter-less Broadcast in Static to highly Mobile (PBSM) ad-hoc networks protocol (Korkmaz et al.), makes use of the DS-NES framework to develop an adaptive algorithm which does not depend on any parameter or threshold value. Due to its flexibility and good performance, it is used as the basis of Broadcast protocol for vehicular ad-hoc networks. In PBSM, each vehicle maintains two lists of neighboring vehicles with respect to the message being disseminated and local one-hop knowledge: R and N, containing neighbors that already received (did not receive, respectively) the message. After a delay time-out, s retransmits the message if the list N is nonempty. Both the list R and N are updated with every copy of message and beacon exchange message received, which may trigger further retransmissions, if N becomes nonempty again. Nodes in the CDS set shorter waiting time-outs than nodes that are not part of it.

2.4 VANET-Specific Broadcasting

limit review to protocols designed primarily for non-safety applications (and therefore not emphasizing minimal delay as the main objective). Vehicles tend to travel forming groups in highly disconnected networks. Vehicular density can be extremely high in a traffic jam, while surrounding streets or lanes could have low traffic density. This uneven node (and speed) distribution is characteristic of vehicular settings. Therefore, several broadcast protocols specifically designed for such networks have been proposed so far.

A few simple geo-casting algorithms are offered in (Lee et al.). Each node periodically broadcasts its query to neighboring nodes. Query is dispersed via mobility and only to one-hop neighbors. It is then extended toward m-hop retransmission similarly (with decreasing hop counter until reaching 0). Next, each receiving vehicle will retransmit with certain fixed probability. Further scheme is random walk to spread the query to k proxy vehicles, and then these vehicles periodically inform their one-hop neighbors. In neighbor split scheme, originator splits k proxy advertisers equally among its neighboring nodes. This continues recursively and then one-hop neighbors are informed periodically. These schemes do not meet satisfactory reliability
In \cite{Sun2010}, two solutions which consider vehicles located in multiple lanes on a highway, all driving in the same direction, are presented. In proposal (sender oriented), the vehicle transmitting the message decides the next forwarder by including the identifier of its farthest neighbor (in the direction of the broadcast propagation) within the message. This approach is not reliable because the intended neighbor might not be reachable when the transmission takes place, since the connectivity was established at a previous beacon message exchange. Such situation would stop the flooding process prematurely. In the second solution, the next forwarder selection is performed at the receiver. The transmitting vehicle appends its own location to the broadcast message. Receivers defer the retransmission for a 'back-off' time which is inversely proportional to their distance from the previous forwarder. In a one-lane highway scenario, the next forwarder is normally the farthest car from the previous forwarder, among those that received the retransmission. This protocol is not intended to guarantee delivery to all nodes. It only discusses progress between two intersections, which is more precisely a small-scale routing task, and not how to retransmit and provide message to nodes between two forwarders. It also is 1D, and messages may 'jump' over intersections. A variant of this scheme has been proposed to implement Cooperative Collision Avoidance (CCA) \cite{Biswas2011}. A 1D broadcasting algorithm to disseminate the same message to all vehicles on a road segment, is described in \cite{Li2010}. As in \cite{Sun2010}, the farthest node from the sender retransmits the message for fast progress. The extension is that, the node closest to the middle, between two senders retransmits for increased reliability. It is not clear how many such iterations are needed, and how this can be extended to 2D scenarios.

Other variants, rely on the MAC layer to improve the broadcasting task in vehicular networks. The Urban Multi-hop Broadcast (UMB) protocol \cite{Korkmaz2010} is an 802.11-based solution targeted at reducing the broadcast storm and Hidden node problems, while maximizing the reliability. The broadcast storm is minimized by only allowing the farthest vehicle which receives a message to forward it. For this, after successfully receiving a message, vehicles issue a black-burst jamming signal, whose duration is directly proportional to the distance between the transmitter and
the receiver. When the signal transmission ends, the vehicle listens to the medium to check if other neighbors are still transmitting a black burst. If not, that vehicle is the farthest one, from the transmitter and forwards the message. The hidden node problem is addressed by adding a Request-To-Broadcast (RTB)/Clear-To-Broadcast (CTB) exchange, similar to the case of uni-cast messages. In addition, reliability is expected to be improved via acknowledgment messages (ACKs, also like unicast). The protocol is designed for dense urban scenarios, with intersections and streets in several directions. Along each street, directional broadcasts take place in the direction of the message propagation. UMB assumes that a repeater is deployed at each intersection, thus initiating directional broadcasts along each of the converging streets. There is also a version of the protocol which substitutes repeaters for regular vehicles which are crossing the intersection (Korkmaz, Ekici, and Uner), therefore eliminating the need of infrastructure.

A highway probabilistic flooding algorithm is proposed in (Nekovee). Front and back counters are updated for received message copies. Before possible retransmission, there is a waiting time that includes the urgency of the message. Probabilistic retransmission decision favors large difference in counters. Upon retransmission, a node sets another waiting time. Cluster merging, balances counters and reduces retransmission probability. The protocol assumes uni-directional traffic only, is probabilistic, and has slow merging, when one counter is already large.

Three probabilistic and timer-based broadcasting suppression techniques for well-connected vehicular networks were proposed in (Wisitpongphan et al.). Their objective was to minimize the well-known broadcast storm problem. In the weighted p-persistence scheme, upon receiving a message, node j waits for a constant time W to receive other potential copies of the message. Let i be the closest neighbor from which the message has been received. Then, j rebroadcasts the message with probability $p_{ij} = D_{ij}/R$ if it receives the message for the first time, and discards it otherwise, where $D_{ij}$ is the distance between i and j and R is the transmission radius. In case j decides to not retransmit, it waits for an additional time $\delta$ (accounts for transmission and propagation delays) to overhear the same message again from any neighbor. If this is not the case, j rebroadcasts with probability 1. In the slotted 1-persistence scheme, j selects time slot $S_{ij} = N_s(1 - \lfloor D_{ij}/R \rfloor)$, where $N_s$ is the
maximum number of slots. It rebroadcast (with probability 1) at the assigned slot, if it receives the message for first time, does not hear any duplicate before the assigned slot; otherwise, the message is discarded. Finally, in the slotted p-persistence scheme, rebroadcasting is done with predetermined probability p instead of probability 1, and retransmission with probability 1 is scheduled if no duplicate was heard within certain time limit. Versions of the algorithms using the Received Signal Strength (RSS), instead of position information, are also described.

The solutions described so far are designed for highway (Sun et al., Biswas, Tatchikou, and Dion), (Wisitpongphan et al.) scenarios. None of them address the issue of temporary disconnections in VANET, which is one of its most salient properties. The Distributed Vehicular Broadcast (DV-CAST) protocol (Tonguz et al.) is the only solution found in the literature, that explicitly addresses the various connectivity conditions, which are present in vehicular networks, although, it can only be applied to rectilinear streets with several lanes (like highways). Vehicle behavior is decided by its status. It is in well-connected status if it has at least one neighbor of the same cluster in the message forwarding direction. In such case, the well-connected vehicle runs one of the broadcast suppression techniques described in (Wisitpongphan et al.). A vehicle is operating in sparsely connected regime if it is the last one in the cluster of vehicles. In addition, it is said to be in a sparsely connected neighborhood if it has at least one neighbor in the opposite direction. Otherwise, the vehicle is in a totally disconnected neighborhood. Upon receiving a message, the sparsely connected vehicle immediately rebroadcasts it. If it moves in the same direction as the original message source, the message is then discarded. Otherwise, the message is carried until it expires or can be retransmitted back to the original message forwarding direction. Message is carried until an implicit acknowledgment is received (from another vehicle with greater hop count), and is being retransmitted, if new neighbors are identified. Vehicle in totally disconnected mode carries the message until a new neighbor is identified, retransmits it with probability 1 immediately, and discards it afterwards.

There are a few drawbacks in the DV-CAST protocol. The notions of neighbor in ‘message forwarding’ and in ‘opposite direction’ may often be unclear, e.g., for highway scenarios with several roads joining at an intersection. Therefore, DV-CAST
will not work in such scenarios. Further, the algorithm also depends on whether or not a sparsely connected vehicle moves in the same direction as the original message source. However, there are scenarios where the message source is static. Next, after a node rebroadcasts the message in totally disconnected mode, it deletes, therefore the next coming neighbors will not receive this message in a scenario where all vehicles on the road are totally disconnected. Finally, after each transmission, neighboring vehicle is assumed to have received it, and there are no attempts to guarantee delivery to all vehicles in the area.

2.5 MAC Protocols for VANETs

MAC layer protocols are responsible for managing and maintaining the wireless channel use. Their main job is to decide which of the nodes should get the channel access and which should wait. There are two managing techniques:

- Contention free, like TDMA, FDMA, STDMA and CDMA, where the need for a central entity is crucial for the fair distribution of the channel resources among the nodes.

- Contention based, or random access protocol, such as the Carrier Sense Multiple Access (CSMA/CA) of IEEE 802.11.

MAC protocols such as TDMA, FDMA, STDMA or CDMA are difficult to implement for vehicular ad-hoc networks (VANETs) since time slots, channels, or codes have to be dynamically allocated. This requires synchronization which is difficult to achieve in high dynamic networks such as vehicular ad-hoc networks (VANETs) (Xu et al.).

To have a reliable and efficient medium access control (MAC) protocol, that suits the high mobility of vehicles, the proposed MAC protocol should avoid transmission collisions between vehicles, hence emergency messages will be forwarded in a real time manner. Moreover the medium (wireless channel) has to be shared efficiently and fairly between vehicles. The transmitted information is usually small, but it has to be propagated to the intended distance in a very short time, usually less than 0.5 seconds as studied by (IntelliDrive). Therefore, the MAC protocol in vehicular ad-hoc networks (VANETs) has to pay more attention to the medium access delay and less attention to the power constraints because vehicles have no power constraints and
2.5. MAC PROTOCOLS FOR VANETS

Figure 2.1: Hidden node and Exposed node

can use global positioning system (GPS) for positioning and time synchronization. Moreover, the proposed MAC protocol should pay attention to the Hidden terminal, Exposed node and capture problems.

The Hidden terminal problem happens when a node is in the range of the receiver but out of the range of the sender. This node cannot hear the transmission from the sender to the receiver. Hence, it may start sending to the receiver at the same time causing collisions as shown in Figure 2.1a. If node A is transmitting to node C, node B is a Hidden Terminal since, it cannot hear the ongoing transmission. Therefore, it may start using the channel, causing a collision at node B. The exposed node problem happens when the node is in the range of the sender but out of the range of the receiver. This node will hear the transmission of the sender to the receiver, therefore it will not use the medium during that transmission while it can transmit to other nodes in its range but out of the range of both the sender and the receiver as shown in Figure 2.1b. If node C is transmitting to node D, node A cannot use the channel although it can transmit to node B without any interference with node D.

The capture problem, occurs when two nodes send data at the same time to another node. One node is closer to the receiver, hence the receiver will decode its data without errors. This will lead to unfairness problem.

Code Division Multiple Access (CDMA) is used between nodes to share a common medium where each node has an orthogonal code to encrypt messages before sending them. Multi-Code MAC (MCMAC) \cite{Jin and Cho} protocol uses one common code for control packets and other codes for data transmission. When the sender wants to initiate a transmission, it sends first RTS message to the receiver encrypted by a common control code, this message includes the data encryption code. Upon receiv-
ing the RTS message, the receiver checks if there is any code conflict with another transmission and replies by CTS message; otherwise it will send the sender its usable codes to select one of them and start the RTS message again. When the sender receives CTS, it starts transmitting the data.

The authors in (Borgonovo et al.) introduce a new MAC architecture called AD-HOC MAC to solve the problems associated with mobile ad-hoc networks and guarantee a relatively good QoS in VANETs. This protocol is developed for the CarTalk2000 project (Morsink and Schulz). This architecture is based on a technique called Reliable Reserved ALOHA (RR-ALOHA) to dynamically assign a single broadcast channel called, Basic Channel (BCH) to every node in the network using slotted or framed structure. The AD-HOC MAC protocol works by grouping the nodes into groups where all nodes are interconnected by broadcast radio communication called One Hop cluster (OH). The main drawbacks of this protocol are that the number of vehicles within the one hop range is restricted to the number of frame time slots and the high overhead ($\geq 25\%$) of dedicating a single control channel for each node in the one hop cluster.

The Dedicated Omni-Purpose Vehicle-to-Vehicle Communication Linkage Protocol for Highway Automation (DOLPHIN) system in (Tokuda, Akiyama, and Fujii) is one of the first V2V Communication protocols and was adopted by the Japanese V2V Communication system to deal with a group of vehicles driving in a platoon. All vehicles in the platoon communicate with each other and send periodic information like speed, direction, and emergency braking of a vehicle to other vehicles in their line of sight (LOS) or route it to the NLOS conditions on vehicles. The platoon in DOLPHIN does not require any fixed infrastructure, since it uses CSMA/CA as the basis for its MAC protocol. The emergency information is allocated the shortest time slot, while other types of information are allocated the larger transmission time slots. This allows the vehicle with critical information to capture the channel before other nodes that have normal information.

Most MAC protocols designs based on IEEE 802.11 standard, use Omni-directional antennas, while using directional antennas will allow VANETs to efficiently use the channel resources. As vehicles are moving in directional roads, directional antennas
2.5. MAC PROTOCOLS FOR VANETS

may help in reducing transmission collisions. The space around each vehicle is divided into \( N \) transmission angles of \( \theta = 2\pi N \) and a separate antenna is responsible for each direction. In Bazan and Jaseemuddin and Michael and Nakagawa, it has been proved that using sector antennas will increase the throughput and only a small increase in received packets is achieved when using more than two antennas. In Young-Bae, Shankarkumar, and Vaidya, the authors proposed a Directional MAC (DMAC) protocol, assuming each node knows its position and the position of its neighbors using GPS. Based on the receivers location, the sender will use one of its directional antennas to send packets to the receiver. The DMAC scheme is based on RTS, CTS and ACK as in IEEE 802.11, except that the ACK is sent using directional antenna instead of Omni-directional antenna. The neighboring nodes that are not participating in the current transmission and upon receiving RTS or CTS by one of its directional antennas will block that antenna during the transmission period specified in RTS or CTS packets.

In Figure 2.2, if node A has a message to transmit to node B, first, it will send a Directional RTS (DRTS). Upon receiving the DRTS, node B will send an Omni-directional CTS (OCTS). A neighbor such as Node C will block its directional antenna that receive the maximum power for duration specified in OCTS. When node A receives OCTS, it will start sending the data. Node B will send an ACK to node A when the transmission is complete.

Most wireless communication standards use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) in IEEE 802.11 to overcome collisions and the hidden terminal problem. The sender will send Request-to-Send (RTS) to the receiver to inform neighbors of the transmission process. The receiver will reply if ready by a Clear-to-Send (CTS) message to the sender. The neighbors upon hearing the CTS, will be aware of the upcoming transmission and will avoid using the channel. After that the sender will start sending the message without any risk of collisions. In the following subsection, the MAC protocol of IEEE 802.11 will be briefly introduced followed by the IEEE 802.11p, which is adopted by the IEEE community as a main technology for VANETs.
2.5. MAC PROTOCOLS FOR VANETS

2.5.1 IEEE 802.11 MAC Layer

The IEEE 802.11, was introduced in 1990 with the interest to develop a wireless LAN operating in the Industrial, Scientific and Medical (ISM) band. Till date the IEEE 802.11 group has issued many standards. The IEEE 802.11a was introduced in 1999 to work in the 5GHz band and using Orthogonal Frequency Division Multiplexing (OFDM) to reach the rates from 6-54Mbps. The IEEE 802.11b is the most accepted standard, introduced in 1999 which uses the ISM 2.4GHz band and Direct Sequence Spread Spectrum (DSSS) to reach rates from 5.5-11Mbps. The IEEE 802.11g uses the same physical layer as IEEE 802.11b but can reach rates more than 20 Mbps up to 54Mbps. The use of the ISM 2.4 GHz unlicensed band increases the interference from other wireless devices like cordless phones, wireless IP cameras and other devices using the same band.

The IEEE 802.11 can work either in a centralized or decentralized mode. An Access Point (AP) is mandatory for the wireless nodes to communicate in the centralized mode, while in the decentralized mode it is not needed (AD-HOC mode).

The availability and the low cost of IEEE 802.11 devices attracted Engineers to implement this technology in the Vehicle-to-Vehicle Communication. The IEEE 802.11
MAC layer covers three functional areas: reliable data delivery, MAC access control and security.

Reliability in the context of VANETs broadcast services is defined as the networks ability for all intended mobile nodes to receive the broadcast messages within specified operation duration. The IEEE 802.11 uses RTS, CTS and ACK to ensure reliability and uses three Inter Frame Spaces (IFS) to control medium access and minimize frame collisions. The Short IFS (SIFS) is the shortest IFS and used by immediate responses like ACK, CTS and Poll response. The Point coordination Function IFS (PIFS), which is the medium length IFS, is used by the centralized controller. The Distributed Coordination Function IFS (DIFS), which is the longest IFS, is used as a minimum delay by all asynchronous frames contending for medium access. The three inter frame spacing intervals are shown in Figure 2.3.

The IEEE 802.11 uses CSMA/CA as follows:

a. First, a node that has data to send will sense the channel. If it is idle, the node waits for a period of DIFS. If the medium is still idle it will send RTS message including its ID and the duration of the whole transmission. Upon receiving the RTS message the receivers neighbors will set their NAV (Network Allocation Vector) to the time indicated in the RTS message and will not use the medium during that time.

b. Upon receiving the RTS message, if receiver is ready, it waits for the time duration called SIFS. If the medium is still idle it will send a CTS message including the transmission duration time. All neighbors receiving this CTS message will set their NAV to the time indicated in the CTS message (the
medium is busy).

c. Upon receiving the CTS message, the transmitter waits for SIFS time before starting the data transmission.

d. When the receiver successfully receives the data, it will wait for another SIFS and sends an ACK only to the sender. All neighbors receiving the ACK message will set their NAV to zero, indicating that the channel is free.

e. If the sender senses the medium as busy, it will wait for a duration of DIFS. If the medium is still busy it will back off a random amount of time before sensing it again. If the medium becomes busy during the back off time then the back-off timer is halted and resumes when the medium becomes free.

f. If the sender did not receive an ACK, it will assume a failed transmission and try to retransmit again.

g. The back-off mechanism used is a binary exponential back-off, that is after every collision, the sender will wait for double the last delay up to a maximum value. Therefore the repeated collisions result in longer waiting times.

In 2007, the IEEE community, published a set of improvements to the MAC layer in IEEE 802.11 standard to enhance the Quality of Service (QoS) for wireless LAN applications. Those improvements enhance the DCF and PCF in the standard 802.11 MAC by introducing a new Hybrid Coordination Function (HCF) which has two methods to access the channel: HCF Controlled Channel Access (HCCA) and Enhanced Distributed Channel Access (EDCA). The IEEE 802.11e (for Information technology) defines Traffic Classes (TCs) in both HCCA and EDCA, hence, the traffic with the high priority wins the contention and waits less time before it is transmitted.

2.5.2 Wireless Access in Vehicular Environments (WAVE)

The IEEE society, has developed a Wireless Access in Vehicular Environments (WAVE) (International) architecture to provide wireless access for vehicular ad-hoc networks. This subsection gives an overview of this architecture following the layered ordering of the open systems interconnection (OSI) model.
In 1997, the Federal Communications Commission (FCC) allocated a bandwidth of 75 MHz in the 5.9 GHz band (5.85-5.925 GHz range) to support the dedicated short-range communications (DSRC) for ITS. In 2004, an IEEE task group (known as IEEE 802.11p (IEEE, “IEEE P802.11p/D5.0 Draft Amendments for Wireless Access in Vehicular Environments (WAVE)")) started developing an amendment to the 802.11 standard for the use of VANETs. Another IEEE group (working group 1609), took the role to develop other OSI layers specifications. There are four documents in the IEEE 1609 standards set: IEEE 1609.1 (P1609.1), IEEE 1609.2 (P1609.2), IEEE 1609.3 (for Information technology), and IEEE 1609.4 (P1609.4). Figure 2.4 shows the WAVE architecture and Table 2.1 lists the services requirements of the IEEE 1609 standards (Jiang and Delgrossi, “IEEE 802.11p: Towards an international standard for wireless access in vehicular environments”). The IEEE 802.11p and IEEE 1609 standards together are called wireless access in vehicular environments (WAVE) since their main goal is to facilitate the provision of wireless access in vehicular environments. Therefore, in the remaining of this thesis, use IEEE 8021.11p, DSRC and WAVE interchangeably.

The WAVE system consists of two units:

a. Roadside units (RSUs), which are installed along the side roads

b. On-board units (OBUs) which are mounted on vehicles.

The standard is intended to allow Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) communications. In this technology, vehicles communicate with each other and the RSUs to form VANETs on the road. VANETs will allow vehicles to send their status and safety messages amongst one another to indicate the presence of accidents and other hazards. In order for these safety applications to run effectively, it is necessary to have a highly reliable Medium Access Control (MAC) layer, such that vital safety messages can be delivered in a timely manner.

The WAVE PHY and MAC layers are based and intended to enhance the IEEE 802.11a, to support the Vehicular Ad-hoc Networks (VANETs) applications. The IEEE group is working on Physical and MAC amendments to the IEEE 802.11, to make it more suitable for the high mobility and fast changing topology of VANETs, where reliability and low latency are crucial. WAVE uses the licensed ITS 5.9 GHz
2.5. MAC PROTOCOLS FOR VANETS

The physical layer of the IEEE 802.11p is a variation of the IEEE 802.11a standard as shown in Table 2.2. Figure 2.5 shows the message structure of the IEEE 802.11p. It employs 64 OFDM sub-carriers where 52 of them are used in actual data transmission. The short and long training symbols located at the beginning of every message are used for signal detection, time synchronization and channel estimation while the guard intervals (GI) are used to eliminate the inter symbol interference (ISI) from the multi-path propagation channel.

The IEEE 802.11p defines up to four EIRP (Effective Isotropic Radiated Power). The maximum power (30W) is reserved for emergency vehicles so that they can reach longer distances to allow drivers to yield the way. The typical safety status messages use the 33 dBm EIRP.

The 75MHz spectrum is divided into seven channels and a 5 MHz guard band. Each channel uses 10MHz frequency bandwidth in contrast to IEEE 802.11a which uses 20MHz to increase its tolerance to the multi-path propagation and Doppler spread
Table 2.1: Operations of WAVE functional entities

<table>
<thead>
<tr>
<th>Entity</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1609.1</td>
<td>Specifies the services and interfaces of the WAVE Resource Manager application</td>
</tr>
<tr>
<td>1609.2</td>
<td>Defines secure message formats and processing</td>
</tr>
<tr>
<td>1609.3</td>
<td>Defines network and transport layer services including addressing and routing support of secure WAVE data exchange</td>
</tr>
<tr>
<td>1609.4</td>
<td>Enables operation of upper layers across multiple channels, without requiring knowledge of PHY parameters</td>
</tr>
<tr>
<td>802.11p</td>
<td>Define the WAVE signaling technique and interface functions that are controlled by the IEEE 802.11 MAC</td>
</tr>
</tbody>
</table>

Figure 2.5: Message structure in IEEE 802.11p

effects in vehicular networks. Using 10MHz channels results in data rates from 3 to 27 Mbps. Figure 2.6 shows the channel allocations in IEEE 802.11p. Channel 178, called the control channel, will be used for safety applications while channels 174, 176, 180 and 182 are service channels and will be used for non safety applications. Two service channels can be combined to form one large channel for certain applications that need large bandwidth. Channels 172 and 184 are dedicated for public safety applications.

Each vehicle will alter between the control channel (CCH 178) and one of the service channels. The control channel of each vehicle will send periodic status messages (beacons), which include its position and status information like speed, acceleration
### Table 2.2: Parameters of the DSRC IEEE802.11p and the IEEE802.11a

<table>
<thead>
<tr>
<th>Parameter</th>
<th>IEEE802.11p</th>
<th>IEEE802.11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data rate (Mbps)</td>
<td>3, 4.5, 6, 9, 12, 18, 24, 27</td>
<td>6, 9, 12, 18, 24, 36, 48, 54</td>
</tr>
<tr>
<td>Modulation</td>
<td>BPSK, QPSK, 16-QAM, 64-QAM</td>
<td>BPSK, QPSK, 16-QAM, 64-QAM</td>
</tr>
<tr>
<td>No. of sub-carriers</td>
<td>52 (48 data &amp; 4 pilot)</td>
<td>52 (48 data &amp; 4 pilot)</td>
</tr>
<tr>
<td>OFDM symbol duration (μs)</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Guard time (μs)</td>
<td>1.6</td>
<td>0.8</td>
</tr>
<tr>
<td>FET period (μs)</td>
<td>6.4</td>
<td>3.2</td>
</tr>
<tr>
<td>Preamble duration (μs)</td>
<td>32</td>
<td>16</td>
</tr>
<tr>
<td>Subcarrier freq. spacing</td>
<td>156.25 KHz</td>
<td>312.5 KHz</td>
</tr>
</tbody>
</table>
Figure 2.6: Channel allocation in IEEE 802.11p

Table 2.3: Contention parameters for IEEE802.11p CCH

<table>
<thead>
<tr>
<th>AC No.</th>
<th>Access Class</th>
<th>$CW_{min}$</th>
<th>$CW_{max}$</th>
<th>AIFSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Background Traffic (BK)</td>
<td>15</td>
<td>1023</td>
<td>9</td>
</tr>
<tr>
<td>1</td>
<td>Best Effort (BE)</td>
<td>7</td>
<td>15</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Voice (VO)</td>
<td>3</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Video (VI)</td>
<td>3</td>
<td>7</td>
<td>2</td>
</tr>
</tbody>
</table>

and direction to the neighboring vehicles. Upon receiving these messages, vehicles will process this information. If any dangerous situation is detected, the vehicle can send a warning message with high priority access class to all other vehicles in the direction of interest for a certain distance to alert drivers to take appropriate and timely action.

WAVE will use CSMA/CA as in IEEE 802.11a and the Enhanced Distributed Channel Access (EDCA) as in the IEEE 802.11e standard as its basic MAC protocol. In this standard, messages are categorized into four different Access Classes:

a. Background

b. Best Effort

c. Voice

d. Video
The contention parameters for the four classes are shown in Table 2.3. Each AC has a separate queue and all four queues will contend internally and the winner message will contend externally with other nodes in the network for accessing the wireless channel.

Each node (vehicle) in IEEE 802.11p network contains these four queues and each queue has different Arbitration Inter-Frame Space (AIFS) which equals to $SIFS + AIFSN_\varrho$ where $\varrho$ is the time slot. The queue with the highest priority has the shortest AIFS and will wait the shortest time before its transmission can start. For the first transmission the node will randomly select a value between $[0 - CW_{\text{min}}]$, where $CW_{\text{min}}$ is the minimum contention window for this access class. This contention window ($CW_{\text{min}}$) will be doubled as $(2(CW_{\text{min}} + 1) - 1)$ each time a collision occurs until the $CW_{\text{max}}$ or the maximum number of retransmissions reached. In case of a collision, the message will be retransmitted after a back-off time. This back-off time is shorter for the high priority traffic. Therefore, the queue with the highest priority will always win the contention of accessing the channel, while other, low priority traffic must back-off and try to retransmit after its back-off time expires.