CONNECTING VEHICULAR NETWORKS TO THE INTERNET: A LIFE TIME-BASED ROUTING PROTOCOL

SAMAN BARGHI

A THESIS
IN
THE DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

PRESENTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF COMPUTER SCIENCE
CONCORDIA UNIVERSITY
MONTRÉAL, QUÉBEC, CANADA

MAY 2009

Library and Archives
Canada

Published Heritage
Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et
Archives Canada

Direction du
Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-63125-6
Our file Notre référence
ISBN: 978-0-494-63125-6

Abstract

Connecting Vehicular Networks to the Internet: A Life Time-based Routing Protocol

Saman Barghi

Inter-Vehicle Communications have recently attracted the attention of researchers in academia and industry. In such networks, vehicles should be able to communicate among each other (V2V) as well as with roadside Infrastructure units (V2I). Vehicular networks try to provide safety on the roads by disseminating critical messages among vehicles. Infrastructure units provide some services such as driver information systems and Internet access. Because of the high speed and high mobility of vehicles, establishing and maintaining a connection to these units is very challenging. We introduce a new protocol that uses the characteristics of vehicle movements to predict the vehicle behavior and select a route with the longest life-time to connect to the wired network. It aims at spreading the advertisement messages through multi-hops without flooding the network, do seamless hand-overs and select the most stable routes to these units. We performed some simulations and compared the performance of our work with some well-known protocols.

Acknowledgments

First, I would like to sincerely thank my hard working supervisor, Dr. Chadi Assi, for all of his support and guidelines during my research and helping me to fulfill my responsibilities toward achieving my goals in my academic life. I also thank Prof. Abderrahim Benslimane for his directions and ideas that helped me acquire great knowledge in my research field. I also would like to thank Dr. J. William Atwood and Dr. Bo Zhu, for accepting to be a member of the defence committee.

Special thanks goes to my lovely mom and dad. I owe everything to them, for all their support, love and encouragement throughout my life.

Contents

List of Figures

List of Tables

List of Publications

- Saman Barghi, Abderrahim Benslimane and Chadi Assi "A Lifetime-based Routing Protocol for Connecting VANETs to the Internet", *10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2009), Kos Island, Greece*

List of Acronyms

AGF	Advanced Greedy Forwarding
AODV	Ad hoc On-Demand Distance Vector Routing
CAR	Connectivity-Aware Routing
CBF	Contention Based Forwarding
CVIA	Controlled Vehicular Internet Access
DHCP	Dynamic Host Configuration Protocol
DREAM	Distace Routing Effect Algorithm for Mobility
DRIVE	DiscoveRy of Internet gateways from VEhicles
DSR	Dynamic Source Routing
DSDV	Destination-Sequenced Distance-Vector
DSRC	Dedicated short-range communications
DYMO	Dynamic MANET On-demand Routing Protocol
EDR	Event Data Recorder
FA	Foreign Agent
GPS	Global Positioning System
GSR	Geographical Source Routing
HA	Home Agent
IETF	Internet Engineering Task Force
IGW	Internet GateWay
IVC	Inter-Vehicular Communication

LAR	Location Aided Routing
LET	Link Expiration Time
LS	Link Stability
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
MIP	Mobile IP
MIPMANET	Mobile IP for Mobile Ad Hoc Networks
MMCS	MIPMANET Cell Switching
MOCCA	MObile CommuniCation Architecture
MOPR	MOvement Prediction-based Routing
MRL	Message Retransmission List
NEMO	NEtwork MObility
NS2	Network Simulator 2
ODAM	Optimized Dissemination of Alarm Messages
PGB	Preferred Group Broadcasting
QoS	Quality of Service
RET	Route Expiration Time
RREP	Route Reply
RREQ	Route Request
SAR	Spatially-Aware Routing
TDMA	Time Division Multiple Access
UMTS	Universal Mobile Telecommunications System
VANET	Vehicular Ad hoc Network
WLAN	Wireless LAN
WRP	Wireless Routing Protocol
WSN	Wireless Sensor Network
ZRP	Zone Routing Protocol

Chapter 1

Introduction

Traffic jams and accidents are wasting a lot of time, money and human lives each year. For example more people have died on Canada's roads in the last 50 years than the number of Canadians killed in two world wars. In fact, the numbers tell us that on average, eight Canadians die in road crashes every day and many more are seriously hurt [1].

In order to make vehicles safer, new features has been added to the vehicles. Airbags, anti lock braking systems and seat belts are examples of such features. However, the number of accidents and injuries did not show a significant change during these years (see figure 1.1)[1].

Most of these problems can be solved, if the drivers receive the appropriate information prior to the accident. Vehicular Ad-hoc NETworks (VANET) were proposed as a solution to reduce the number of accidents and traffic on the road, and provide safety for the vehicles and the passengers. By using such networks, vehicles will be able to send the safety information to each other and prevent the accidents from happening. Emergency notification, congestion detection, collision alert, obstacle warning and intersection collision warning are the services provided by such networks. For example, in case of an accident, vehicles on the scene can inform

[1] Transport Canada [1]

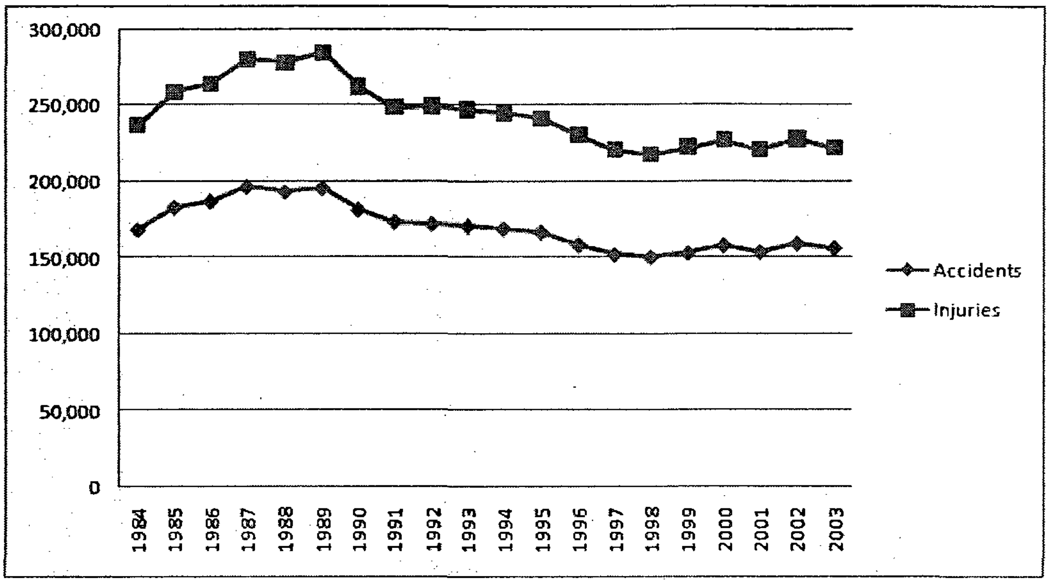


Figure 1.1: Change in number of accidents and injuries during the past years

other vehicles to slow down or change their lanes, to prevent further accidents from happening. Other example can be updating the drivers about the traffic information to help them avoid the traffic congestion and select a better route towards their destination.

Besides providing safety for vehicles, vehicular networks can be used to provide information and entertainment for the passengers. For example, they can be used to provide Internet access, mobile advertising and support for vehicle platoons.

1.1 Overview of Vehicular Networks

VANET is the largest implementation of Mobile Ad-hoc Networks [2] in which vehicles on the road are the mobile nodes. VANET and MANET have similar characteristics and some differences. High mobility of the vehicles, fast topology changes, frequent fragmentation in the network and scalability are new challenges introduced by VANET. Sharing the same channel by vehicles will lead to congestion in very dense networks. Besides, since vehicle movements are constrained by the roads (streets and highways), their movements are predictable. In addition, since all the equipment is located inside the vehicle there is no limit for the power supply, storage and computing resources.

Other than the multi-hop behavior of vehicles in VANET, vehicles will exchange the information they receive from their radars and sensors deployed in the vehicle. In this case, VANET is similar to Wireless Sensor Networks (WSN) [3]. In such networks nodes receive some information about their environment by using integrated sensors in the system in a decentralized manner. VANET and WSN both can use data-centric routing approaches to eliminate redundancy, minimize the number of transmissions and improve the quality of the sensor information. However, sensor networks are not mobile and again there are some constraints on power and capability, which is not an issue in VANET.

In general, there are three possible communication approaches for Vehicular Networks [4]:

- **Mobile Ad-hoc Networks:** These networks consist of mobile devices that are interconnected to achieve unicast or multicast communication similar to fixed networks in the absence of infrastructure.

- **Wireless Sensor Networks:** A Wireless Sensor Network [3] typically consists of a number of immobile sensor nodes each equipped with a sensing device, micro-controller, radio transceiver and power supply. The task of the network is to perform distributed measurements and to transfer these to one or more sinks for analysis and interpretation.

- **Infrastructure-based wireless networks:** Infrastructure-based networks provide a mobile user with different network services by means of a fixed infrastructure. In such networks, only the last hop is wireless, the user communicates directly with the nearest station. Examples are mobile phone systems (GSM [5], UMTS [6], IMT-2000 [7]) or the well-known 802.11 WLAN [8].

Infrastructure-based networks are more mature than the previously described networking technologies. They are already in productive use, offering popular services such as telephony, text messaging or data transmission. These networks typically support unicast, but some are also able to provide multicast and broadcast communication [4].

Taking these communication possibilities into consideration, there is a strong need to develop new system concepts and information dissemination protocols for VANET. Some issues concerning architecture, security, routing, performance or QOS need to be investigated. These newly developed protocols should be carefully standardized to support inter-operability, in order to provide a smooth connection between vehicles from different vendors.

For connecting vehicles to each other in a VANET, at first all the efforts were concentrated on creating a scalable ad hoc routing protocol that is able to deliver all the messages in a timely manner, and support point-to-point communication between vehicles. Following this theory, the best way to disseminate alarm messages in VANET is using packet broadcasts to inform other vehicles about the events or road conditions. However, it is not easy to design a protocol to support the point-to-point communication between the vehicles in such a dynamic and large scale network. For instance, if two vehicles that are separated by ten vehicles in the network, want to communicate through multiple hops, the delay and loss rate will be dramatically high. To resolve this issue, a vehicle should use the ad-hoc networks just to communicate with its neighbors, and use the infrastructure units to communicate with the vehicles far apart or to receive other services such as Internet access.

The first step on the road to the standardization process was taken by US Federal Communications Commission by allocating 75 MHz (from 5.850 to 5.925

GHz) of DSRC (Dedicated Short Range Communications) [9] spectrum to accommodate Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication for safety-related applications. It is based on IEEE 802.11 and provides a very high data transfer rates in circumstances where minimizing latency in the communication link and isolating relatively small communication zones are important.

Another interesting area of research in VANET that attracted a lot of attention is routing. MANET routing protocols can be used in VANET to handle the multi-hop nature of VANET. However, most of the ad-hoc routing protocols are not able to handle a large number of vehicles and fast topology changes in VANET. Reactive, proactive and position-based routing protocols are different ad-hoc routing protocol categories among which geographical routing is more appropriate for VANET. Vehicles in VANET are equipped with a positioning system, e.g., GPS (Global Positioning System) in order to obtain location information. Different approaches for routing the packets in VANET network will be discussed in the following chapter.

Security and Privacy are issues that need to be carefully investigated and addressed in the design of the communication protocols in VANET. Several threats including bogus traffic information, fake messages to generate "Intelligent collisions", cheating with Identity and position, and jamming should be addressed before this network becomes functional. Privacy also should be take into consideration, anonymity of the drivers and passenger information and actions are required. Moreover, no one should be able to track the vehicle by using the information transmitted among vehicles [10].

1.2 Motivations and Preliminaries

Without any doubt, the Internet has changed the way we live and work, and it became a very important part of the modern life. People can access the Internet from their office or home networks, through available hot spots or by using their cell phones. However, it remains difficult to have high speed Internet access while driving on the road, which seems to be necessary as the Internet usage continues to grow.

In vehicular networks, Internet access is provided through the gateways that are implemented into roadside infrastructure units, which enable vehicles to communicate with the outside world. These gateways, called Internet edges, are part of the Internet as well as the vehicular network. The multi-hop nature of VANET makes it challenging for vehicles to find a gateway and select the best one. Further, as a vehicle moves, it needs to find new gateways along the road and hand-over the connection from the previous gateway to the new one in order to remain connected.

Indeed, high mobility and fast topology changes make it hard to build robust and stable routes to gateways; nonetheless, Internet access should be available independent of the vehicle location. In order to connect to the Internet, each vehicle should have a unique static IP address; this will help to route the packets from, and to these vehicles. Mobile IP [11, 12] is a solution to provide static global IP addresses to mobile nodes and handle the mobility, however it requires that mobile hosts be one hop away from foreign agents deployed in the gateways. Thus, the challenge that faces connecting vehicular ad hoc networks to the Internet is extending Mobile IP to manage node mobility even when these nodes are multiple hops away from the edge of the Internet.

Additionally, the high speed of vehicles may cause frequent fragmentation in the network, which should be transparent to users. Connections should also be seamlessly handed over to the next gateway before the current connection terminates. For this purpose, vehicles have to be informed about the alternative gateways prior to connection termination, to be able to communicate with them. Now, the large number of vehicles on the road brings up some other challenges as well; e.g., IP

Broadcasts can flood the network quickly and cause extra overhead, and create scalability problems. To overcome these limitations, we propose a new approach to discover gateways.

Since the vehicles are constrained by the existing highways, streets and roads, their movement is to some extent predictable. This feature can be used to predict vehicle behaviors prior to happening, e.g., it can be used to predict the future vehicle location or link life-time. We will benefit from this feature in the design of our protocol, which will be explained later.

1.3 Thesis contribution

The objective of this work is to design a new protocol to provide Internet access for the vehicles that reduces the overhead during the gateway discovery process, selects the most stable route and performs seamless hand-overs. We will use a hybrid gateway discovery process, restricting broadcasts to a pre-defined zone and let only some relays to be able to re-broadcast the advertised messages. We modified the Contention Based Forwarding (CBF) [13] protocol in order to spread the gateway advertisement messages among the vehicles. We also use stability metrics (e.g., speed, direction and location) of vehicles to predict the link life-time, and recursively the life-time of a route from a vehicle to a gateway. We use this information to select the most stable route from vehicles to gateways. The most stable route is not necessarily the shortest one, it is the path with the longest life-time. Here we are more interested in the life-time of the connection rather than the number of hops to the destination, in order to make the links more robust.

Having a list of routes to different gateways, a vehicle can hand-over the connection to the next available gateway before the current connection fails. If a vehicle does not receive advertisement messages, it should start sending out solicitation messages to find a new gateway. In this work we present a framework for connecting VANET to the Internet, that is based on the estimation of the link life-time and stability of the links. We performed extensive simulations and compared our protocol to Ad hoc On-Demand Distance Vector Routing (AODV) [14] and Greedy Perimeter Stateless Routing (GPSR) [15]. The results of the simulations shows that our protocol performs better in terms of packet delivery ratio and packet delivery delay.

1.4 Thesis Outline

The rest of this thesis is organized as follows: Chapters 2 and 3 focus on reviewing ad-hoc and VANET routing protocols and investigate the different approaches to provide the Internet access for these networks. In Chapter 4, we explain our approach to integrate vehicular networks to the Internet. In chapter 5 we evaluate the performance of our protocol, and chapter 6 concludes and provides direction for future work.

Chapter 2

Background and Related Work: Mobile Ad-hoc Networks (MANET)

VANET is the largest implementation of MANET, in which vehicles are the mobile nodes. However, most of the existing MANET protocols cannot be used in VANET scenarios because of the scale, speed of the nodes and the fast topology changes in such an enviornment. In spite of these problems, it is necessary to fully understand the Ad hoc Network protocols and architecture before one moves to the VANET. For this purpose, we first review the mobile ad hoc networks in this chapter and then describe VANET and its features in the next chapter. In this chapter we will provide a review on Mobile Ad-hoc Networks, existing routing protocols and different approaches to connect ad-hoc networks to the Internet.

2.1 Outline

This chapter is structured as follows: In section 2.2 we review Mobile Ad hoc Networks in general. Section 2.3 covers different MANET routing protocols. In section

2.4 we give an overview of Mobile IP, and in section 2.5 different approaches to connect MANET to the Internet are discussed. Section 2.6 presents the conclusion and discuss the disadvantages of using MANET protocols.

2.2 Introduction

Mobile Ad-hoc Networks consist of mobiles nodes that can move randomly, and at the same time they have the ability to communicate with each other. These networks are not dependent on any infrastructure and are completely self-organized. A node can be a host and a router at the same time, and they can communicate with the nodes that are not directly connected to them through multiple hops. Messages and Packets are transmitted in a store-carry-forward manner. It means that when a node receives a packet it checks whether the packet is destined for it or not. If so, it will keep the packet, otherwise the packet will be stored and based on the routing policy, it will be forwarded to the next hop until it reaches the destination.

Wireless nodes in an ad hoc network can communicate with other nodes that are immediately in their radio range or the nodes that are outside of their range. Intermediate nodes are responsible for forwarding the packets between a sender and the receiver if they can not communicate directly. For instance, if two nodes are separated by an obstacle, other nodes can deliver the packets between these two nodes.

In MANET, nodes move freely and their movements are not predictable. This dynamic behavior causes some changes in the topology over time. These changes must be known to all the nodes in the network, and the topology information should be updated accordingly. Ad hoc networks are completely autonomous and there is no need for any administration. However, they can be connected to an infrastructure to receive some services such as Internet access.

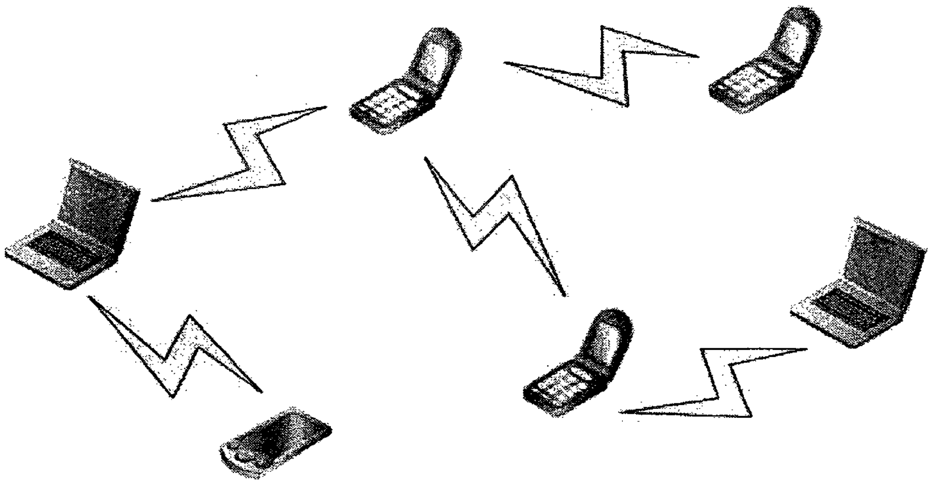


Figure 2.1: Different types of network devices that can exist in an ad hoc network.

Wireless nodes that take part in an ad hoc network can be of any type. Cell phones, laptops, personal digital assistants and many other types of digital devices with communication facilities can be part of an ad hoc network (Figure 2.1). Each of these devices has different computing, communication and storage capabilities and also the battery is limited in some cases. As a result, it would not be enough to only discover the neighbor in an ad hoc network, the information about the *type* and *attributes* of the neighbor seems to be required as well.

Lack of centralized control and global synchronization in ad hoc networks causes TDMA and FDMA schemes to be unsuitable for such networks. Medium Access Control (MAC) protocols are responsible for coordinating the access from active nodes. The wireless communication channel is prone to errors and problems such as the hidden-terminal problem, the exposed-terminal problem, and signal fading effects [16]. Therefore, MAC protocols play a significant role in wireless networks. Authors in [16] stated the problem and investigated the existing solutions and provides a list of available MAC protocols for ad hoc networks.

2.3 Routing in Mobile Ad-hoc Networks

Routing in MANET is utterly different from routing in infrastructure based networks. Dynamic topology, limited network capacity, energy constrained nodes, variable wireless link quality, interference and selection of routes are all challenges to design routing protocols in such networks [17, 18].

Nodes in a MANET require reachability information about their neighbors in order to be able to route the packets, however, the network topology is changing frequently and nodes need to update their information and stay tuned. Besides, some networks (e.g., military networks) can be relatively large, therefore, finding a route to a destination requires exchanging a lot of routing information among the nodes. As a result, the designed routing protocols need to be scalable. In other hand, high mobility nodes will cause the topology to change more frequently, and therefore impose higher overhead on the network in a way that no more bandwidth will remain for transmission of data packets [19].

There are two different approaches for routing in MANET: *topology-based* and *position-based* routing [20]. Topology-based routing protocols use the information about the links that exist in the network to perform packet forwarding. They can be further divided into *proactive*, *reactive*, and *hybrid* approaches. Position-based routing algorithms uses additional information about the position of the nodes to route the packets. Detail information about each approach comes in the sequel.

2.3.1 Topology Based Routing Protocols

Topology-based routing algorithms use the information about the existing links and current network topology for routing the packets in MANET. Proactive, reactive and hybrid approaches are different topology-based routing protocols, which will be explained shortly.

Proactive routing (table-driven) requires that all the nodes keep track of routes to all the possible destination even if they are not used. Therefore, the route to each destination is already known, and a received packet can be forwarded immediately. In these approaches, nodes are periodically sending out some information about their state to update other nodes, and also each node keep a table of possible routes to other nodes. The advantage of this approach is that the delay will be minimum since nodes will simply look up their routing table and forward the packets with no delay. However, routing information will use a large amount of the network capacity if the network topology changes frequently or when the number of nodes is large.

Destination-Sequenced Distance-Vector (DSDV) [21] is a proactive distance vector routing protocol that requires each node to periodically broadcast routing updates. Each node maintains an incrementing sequence number that will be incremented each time the nodes sends out the update information. This sequence number is used to differentiate between fresh and expired routes. The latest sequence number is always used to update the routes and if the sequence numbers are equal the one with smallest distance metric is used. DSDV avoids long-live loops and count to infinity problems.

Wireless Routing Protocol (WRP) [22] is a proactive unicast routing protocol for MANET. WRP uses improved Bellman-Ford Distance Vector routing algorithm. Using WRP each node maintains four tables: Distance table, routing table, link-cost table and a Message Retransmission List (MRL). Routing table keeps the information about the destination, the predecessor and successor along the paths to the destination and tags it as simple path, loop or invalid based on the state of the route. Link-cost table holds the information about the neighbors and the cost of the link for connecting to the neighbor. Nodes will exchange their routing tables with their neighbor by sending update messages. This messages can be sent periodically or whenever a link state changes happen. MRL table keeps track of the neighbor that have not sent an acknowledgment back, and if necessary the update message will be retransmitted. If no change happens, each node send out a hello message to ensure the connectivity. When receiving an update message each node modifies its distance table and checks if there is a better route available according to new information. WRP avoids loops and count to infinity problem that can be found in original distance vector routing algorithms. However, WRP requires large storage and computing capacity to maintain various tables.

Reactive routing (on demand) was introduced to avoid the shortcomings of proactive routing protocols. These protocols maintain routes "on demand". Thus when a route is needed the source node starts a route discovery process to find the proper route to the destination. In this case, the network will not be flooded with unnecessary routing information about the routes that are not required. However, before establishing a connection a route discovery process should be performed before the peers can exchange any packets. In addition, reactive routing protocols can still generate a considerable amount of traffic when the network topology changes frequently. On the other hand, packet loss may occur if the route to destination changes during the transmission.

Dynamic Source Routing (DSR) [23] is a reactive routing protocol in which nodes exchange the information based on the paths stored in source routes carried by the data packets. DSR consists of two levels: route discovery and route maintenance. When a node wants to send out a packet it initiates a route discovery process by broadcasting a route request packet. This request contains destination and source addresses along with an identification number. Each node upon receiving this request will check whether it has a route to the destination or not, if not it adds its own address to the packet forwards it along its outgoing links. When a node finds such a route it will send back a route reply along the route from which the route request came. Route maintenance uses acknowledgments and error packets in order to maintain the state of each route.

Ad hoc On Demand Distance Vector (AODV) [24] is an on demand routing protocol that uses route requests (RREQ), route replies (RREP) and route error (RERR) messages for route discovery and maintenance. It uses sequence number to make sure that the routes are fresh, it is loop-free, self-starting and scales to large number of nodes. When a node wants to transfer some information to a destination, it initiates a route discovery process by broadcasting a RREQ packet to its neighbors. During this process, intermediate nodes record the address of the neighbor, from which they received the first copy of the RREQ packet, in their routing table. Once a route to the destination found, the last node will respond by sending back a RREP packet to the neighbor from which it received the RREQ packet. RREP will be routed along the reverse path until it reaches the source node, intermediate nodes will record the forward route entries in their routing table. If a node moves, it can re-initiate the route discovery process to find a new route to the destination. However, if a route in the middle of the route fails, the upstream neighbor will notice and propagates a link failure message to each active upstream neighbors. Nodes will propagate this failure messages until they reach the source node, the source node may initialize the route discovery process if it is still required.

Hybrid routing protocols are a combination of proactive and reactive routing protocols. They benefit from the advantages of both approaches. For example, a protocol may utilize a proactive routing approach for a cluster of nodes and outside of this cluster mobile nodes have to discover new routes on demand. Inside the cluster the delay is minimum and since the packets are not broadcasting outside the cluster, overhead is not a big issue anymore.

Zone Routing Protocol (ZRP) [25] is an example of hybrid routing protocols that divide mobile nodes to different zones, using a proactive routing approach inside a zone and a reactive routing protocol outside the zone and between two zones. The

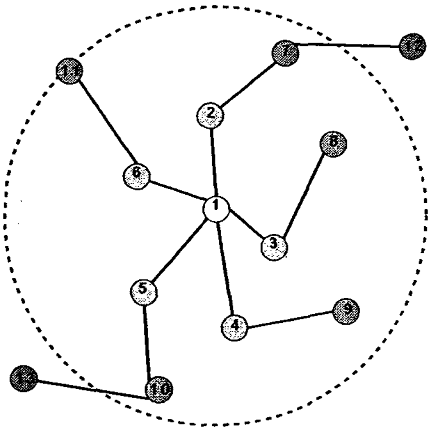


Figure 2.2: Routing zone of node 1 where the zone radius is set to 2 hops.

routing zone of a node will be a set of nodes whose minimum distance in hops from the node in question is no greater than a parameter referred to as the *zone radius.* Figure 2.2 illustrates the routing zone of node 1 where the zone radius is set to 2. Nodes, 2-11 are in the routing zone of node 1, and nodes 12 and 13, 3 hops away from node 1, are not in the zone. Each node in the network has a zone around it, inside which the beacons broadcast from that node will be spread. In this way, the overhead from broadcast messages will be a small and network will not be flooded with broadcast messages from different zones. Inside this zone, proactive routing protocol is being used and all the nodes inside this zone can route packets to node 1 by looking up their routing table. However, if a node wants to send a packet to node 1 and the node is outside the routing zone, it has to send a route request to find a route to node 1. When this request reaches one of the nodes that are inside the zone, they will send a reply back to the source node and inform it about the existing route. In this way, the amount of time required to find a route will be kept small since the nodes inside the zone already have a route, and nodes outside the route will save some time during this process since reaching one of the nodes in the zone is enough to find a route to the node that is the center of the zone.

2.3.2 Position-Based Routing Protocols

Position-based routing algorithms use additional information about the position of participating nodes. These information can be determined using Global Positioning System (GPS) or other positioning services. In order to determine the position of the destination and to include it in the packet's destination address, a *location service* is used by the sender of a packet. Each node routes the received packets based on the position of the destination contained in the packet and the position of the forwarding node's neighbors. Therefore, there is no need to store routing tables or to transmit messages to keep such tables up to date [20]. In addition, such routing approaches are able to deliver the packets to all nodes in a given geographic region, which is called *geocasting* [26].

It has been confirmed [27, 28] that topology-based routing protocols such as AODV, DSDV, or DSR are not scalable. Scalability in Ad hoc networks have significant importance, and routing protocols should be able to manage large networks as well as small networks. However, position-based routing algorithms, as mentioned earlier, do not broadcast control messages and do not keep routing tables, thus their performance does not change significantly in large scale networks. In addition, such protocols use *localized* routing algorithms to route packets globally. In a *localized* routing algorithm, each node just decides to which neighbor it should forward the message, based solely on the location of itself, its neighbors, and the destination. However, in non-localized algorithms, each node maintains accurate topology of the whole network. Also using local information results in less overhead in position-based routing approaches, since nodes only require the position information of neighbors and the destination.

Some position-based routing approaches include the exchange of location information as part of their protocols (e.g., DREAM [29] and LAR [30]). However, most of the position-based routing protocols assume that location information is provided through a separate mechanism. These information are provided by a *location service* to the nodes in a network. There are two general types of location services: proactive and reactive location services. In proactive location services, nodes exchange location information periodically. In contrast, reactive location services query location information when needed. Study of different location services is out of scope of this work, however, a survey of protocols that provide location information for an ad hoc network is available in [31].

Different qualitative characteristics for position-based routing algorithms are listed below [32]:

loop-freedom. The proposed routing protocols should be inherently loop-free to avoid timeouts.

Distributed Operation. As explained earlier, *localized* algorithms are distributed algorithms in which each node makes decisions to which neighbor forward the message based solely on the location of itself, its neighboring nodes, and destination. *Global* approaches, however, assume that each node knows the position of every other node in the network, in addition to the sleep and active periods of each node. Routing using global algorithms is equivalent to the shortest path problem, if hop count is used as the main performance metric. Between these two approaches, *zonal* approach divides the network into zones with localized algorithm applied within each zone, and shortest path or other scheme is applied for routing between zones.

Path strategy. The shortest path route is an example of a *single path strategy*, where one copy of the message is in the network at anytime. On the other hand, *flooding* based approaches flood the messages through the whole network area. However, in *multi-path* strategy, routes are composed of few single recognizable paths.

Metrics. *Hop count*, which is the number of transmissions on a route from a source to a destination, is used in most routing schemes. However, if nodes can adjust their transmission power (knowing the location of their neighbors) then the constant metric can be replaced by a *power* metric that depends on the distance between nodes. The *cost* metric (a rapidly increasing function of decreasing remaining energy at node) is used with the goal of maximizing the number of routing tasks that network can perform.

Memorization. Some solutions require nodes to memorize route or past traffic. These solutions are sensitive to node queue size, changes in node activity and node mobility while routing is ongoing.

Guaranteed message delivery. The primary goal of every routing scheme is to deliver the message, and the best assurance one is to design routing scheme that will guarantee delivery.

Scalability. Wireless networks can consist of a large number of nodes, this makes it necessary for routing strategies to be scalable. However, scalability is sometimes judgmental and is dependent on performance evaluation outcome.

Robustness. The use of position of nodes for routing poses evident problems in terms of reliability. The accuracy of destination position is an important problem to consider.

We divide position-based routing protocols in three categories based on different forwarding strategies they use [20]: greedy packet forwarding, restricted directional flooding and hierarchical routing. Here, we will just discuss the greedy packet forwarding and restricted directional flooding approach, more information can be found in [20, 32, 33].

Using **Greedy packet forwarding**, the approximate position of the destination is included in the packet by the source node. This information is gathered by an appropriate location service, and an intermediate node will forward the received packet to a neighbor that lies in the general direction of the destination. Nodes will forward the packet until it reaches the destination.

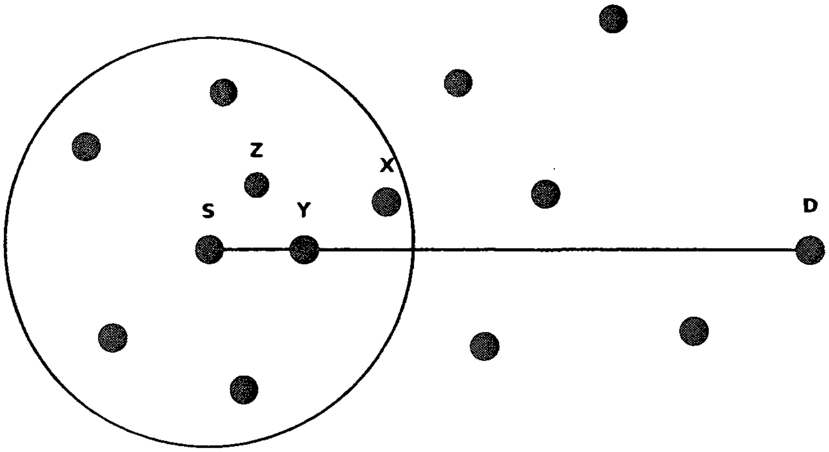


Figure 2.3: Different types of greedy routing forwarding strategies.

Different strategies can be used by a node to decide to which neighbor it should forward the packet. The first strategy is to forward the packet to the node that makes the most progress towards the (is closest to) destination, which is known as *Most Forward within R (MFR)* [34]. In figure 2.3, node S is the sender, and D is the destination. If S uses MFR approach to forward the packets, the next hop in the route will be node X, since it is the closest neighbor of S to destination D. This approach tires to minimize the number of hops a packet has to traverse in order to reach the destination. MFR performs well whenever the sender of a packet cannot adapt the signal strength of the transmission to the distance between sender and receiver.

Nearest with Forward Progress (NFP), in the other hand, is based on the transmission of the packet to the nearest neighbor of sender that is closer to the destination, which is node Z in figure 2.3. This approach is useful when the sender can adapt its signal strength and will help nodes to keep their energy consumption low. *Compass* *routing* is another strategy, which selects the neighbor closest to the straight line between sender and destination [35], node Y in figure 2.3.

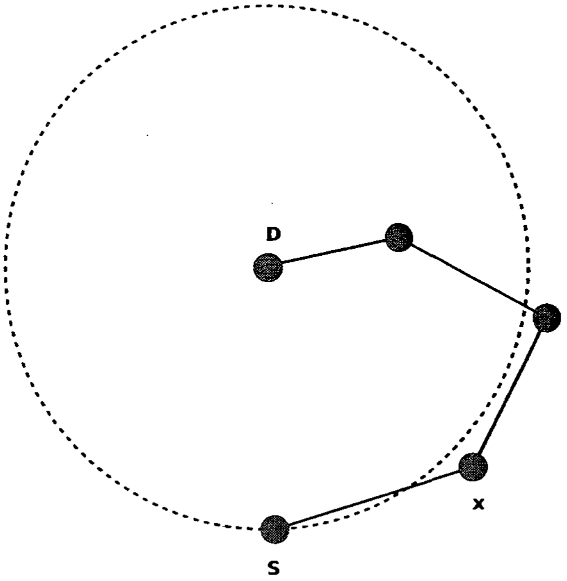


Figure 2.4: Greedy forwarding failure and recovery.

Unfortunately, the greedy forwarding approach may fail to find a path between the sender and destination, even though one does exist. For instance, figure 2.4 shows an example where node S is a local maximum in its geographic proximity to D; x is farther from D, therefore x will not find a path towards the destination, whereas one exists. To counter this problem, it has been suggested that the packet should be forwarded to the node with the least backward (negative) progress [34], if there is no node in the forwarding direction. However, this causes the looping problem that can be solved if do not forward the packets that reached a local maximum at all.

Greedy Perimeter Stateless Routing Protocol (GPSR) [36] is a greedy algorithm using recovery approaches and is based on planar graph traversal. GPSR does not require nodes to store any additional information, and is performed on a per-packet basis. A packet is forwarded using a greedy forwarding based on MFR strategy which means it forwards the packets to nodes that are always progressively closer to the destination. If such a greedy path does not exist, GPSR recovers by forwarding the packet in the *perimeter mode*, in which a packet traverses successively closer *faces* of a planar subgraph of the full radio network connectivity graph, until reaching a node closer to the destination, where greedy forwarding resumes.

In GPSR, nodes send their positions along with their IP address, by broadcasting beacons periodically. This strategy provides all the nodes with the position information of all the neighbors. If a node does not receive any beacon from a node, it will delete this node from its table after a predefined time interval. If the greedy approach fails to find a path to the destination, GPSR starts to use the right-hand rule (perimeter) to traverse the graph and find a route to the destination. This rule states that each node while receiving the packet will send the packet to the first neighbor counterclockwise about itself.

Contention Based Forwarding [13] is a greedy forwarding scheme that does not utilize position beacons to determine the next-hop node. In CBF, the forwarding node transmits a packet including the destination location as a single-hop broadcast to all neighbors and the neighbors contend to forward the packet. The neighbors set up random timers based on how much progress the neighbor will provide the packet to the destination. The timer for the node with the largest progress to destination will expire first and that node will forward the packet. Upon hearing the packet transmission, other neighbors will suppress their packet transmission. There are suppression alternatives to reduce the area from which the next-hop node is selected and to reduce packet duplication caused by neighbors that are within transmission range of the sending node but not of all other contending nodes. This protocol will be explained in detail in chapter 4, since our approach is based on some functionalities in this protocol.

Restricted directional flooding is similar to greedy forwarding strategy in the way that it forwards the given packet to the nodes one hop away from the source node.

However, the difference is that they do not unicast the packet but multi cast it to all the nodes that are closest to the destination than themselves.

Distace Routing Effect Algorithm for Mobility (DREAM) [29] is a restricted directional flooding. In DREAM the sender S of a packet with destination D will forward the packet to all one-hop neighbors that lie "in the direction of D". In order to determine this direction, a node calculates the region that is likely to contain D, called the expected region. Since this position information may be outdated, the radius r of the expected region is set to $(t_1t_0) \times vmax$, where t_1 is the current time, t_0 is the timestamp of the position information S has about D, and $vmax$ is the maximum speed that a node may travel in the ad hoc network. The neighboring hops repeat this procedure using their information on Ds position. If a node does not have a one-hop neighbor in the required direction, a recovery procedure has to be started. This procedure is not part of the DREAM specification.

Location Aided Routing (LAR) [30] is another restricted directional flooding algorithm that does not define a location-based routing protocol but instead proposes the use of position information to enhance the route discovery phase of reactive ad hoc routing approaches. Reactive ad hoc routing protocols frequently use flooding as a means of route discovery. Under the assumption that nodes have information about the position of other nodes, this position information can be used by LAR to restrict the flooding to a certain area. This is done in a fashion similar to that of the DREAM approach.

When node S wants to establish a route to node D, S computes an expected zone for D based on available position information. If no such information is available LAR is reduced to simple flooding. If location information is available (e.g., from a route that was established earlier), a request zone is defined as the set of nodes that should forward the route discovery packet. The request zone typically includes the expected zone. Two request zone types have been proposed: The first is a rectangular geographic region. In this case, nodes will forward the route discovery packet only if they are within that specific region. The second is defined by specifying (estimated) destination coordinates plus the distance to the destination. In this case, each forwarding node overwrites the distance field with its own current distance to the destination. A node is allowed to forward the packet again only if it is at most some δ (system parameter) farther away than the previous node.

2.4 Mobile IP

Since Mobile IP [37] is an important part of the protocols designed to connect ad hoc networks to the Internet, and it supports the mobility of nodes. Here, we give an overview of Mobile IP to make it easier to understand the next section. Mobile IP was designed by the IP routing for Wireless/Mobile Hosts working group of the Internet Engineering Task Force (IETF). The objective of Mobile IP is to route packets to mobile nodes at the network layer. Mobile IP defines three functional entities:

- Mobile node: A node (or host), that changes its point-of-attachment to the Internet from one link to another while using the same IP address.
- Home agent: A router that has an interface on the mobile node's home link. It keeps track of the current location of the mobile node, intercepts packets destined to the mobile node's home address, and tunnels them to the mobile node's current location.
- Foreign agent: A router that has an interface on the mobile node's foreign link (or link visited by the mobile node). It acts as a default router for the mobile node's generated packets. It also de-tunnels packets tunneled by the home agent and destined to the mobile node.

Every mobile node has a permanent IP address, called its home address, which is related to the mobile node's home agent. One of the requirements for Mobile IP is to allow a mobile node to communicate with other nodes using only its home address regardless of its point-of-attachment to the Internet. On its foreign link, a mobile node is assigned a care-of address, which informs the home agent about the current point-of-attachment of the mobile node. A mobile is required to register its care-of address with its home agent. The home agent will tunnel any packet destined to its mobile node using its care-of address. Home and foreign agents advertise their presence through agent advertisements. A mobile node can also discover agents by sending agent solicitations, which will force any agent on the link to reply with agent advertisements.

Mobile IPv6 [11] provides some improvements over Mobile IPv4. First of all, IPv6 has a larger address space than IPv4, which leads to more efficient deployment of MIPv6 in large environments. Second, MIPv6 implements optimized routing, thus eliminating the "triangle routing" problem in MIPv4. The triangle routing means that packets sent by a correspondent node should be first sent to the mobile node's home agent, which will tunnel them to the mobile node's care-of address. Packets sent by the mobile node, however, are transmitted directly to the correspondent node. The optimized routing allows the correspondent node to send its packets directly to the mobile node's care-of address, thus bypassing the mobile node's home agent. Third, the notion of foreign agent does not exist in MIPv6. Fourth, MIPv6 uses IPsec as its security mechanism[1].

2.5 Internet Access in Ad-hoc Networks

Nodes in Ad hoc networks can be connected to the Internet over multiple hops. In this way, users can roam from one wireless network to the other one while they are

[1] Mobile IP overview was taken from [38]

stay connected to the Internet. However, roaming in hierarchical IP networks, which assign IP addresses in a hierarchical way, creates some problems. Nodes that are roaming between base stations or from one network to another are required to have a fixed IP address in order to be able to continously stay connected. As a solution for connecting mobile nodes to the Internet, Mobile IP [11, 12] is widely accepted. Mobile IP allows mobility support based on IP addressing and packet forwarding. Handoff latency results in packet losses and severe end-to-end performance degradation. In order to mitigate these effects, various Mobile IPv6 extensions have been designed to augment the base Mobile IP with hierarchical registration management, address pre-fetching and local retransmission mechanisms (Hierarchical Mobile IPv6 with Fast-hand-over [39], Mobile IPv6 with Fast-hand-over [40], Simultaneous bindings [41], and Seamless handoff architecture for Mobile IP (S-MIP) [42]).

Connecting ad hoc networks to the Internet requires that some nodes (stationary or moving) be part of the ad hoc network as well the Internet. These nodes, called gateways, are equiped with two interfaces, one connected to the Internet and the other one connected to the MANET using the running ad hoc routing protocol. Mobile IP foreign agents are also implemented as a part of the gateway, and gateways are allowing these agents to forward the messages sent from the Internet to MANET nodes. The list the different appraches to connect ad hoc networks to the Internet follows.

HM Ammari in [38] classify the existing approaches into different categories based on two criteria, which is related to the type of architecture of the hybrid network. This higher classification leads to two-tier and three-tier architectures. Connecting MANETs to the Internet strongly depends on Mobile IP and ad hoc routing protocols, which are used to facilitate interactions between MANET nodes and the Internet. Furthermore, the discovery process of the gateways and their selection are considered as criteria to produce a finer classification of the proposed approaches.

2.5.1 Two-tier Architectures

This architectures consists of two layers: first one includes Mobile IP foreign agents, which act as access points to the Internet, while the second one contains MANET nodes desiring Internet access.

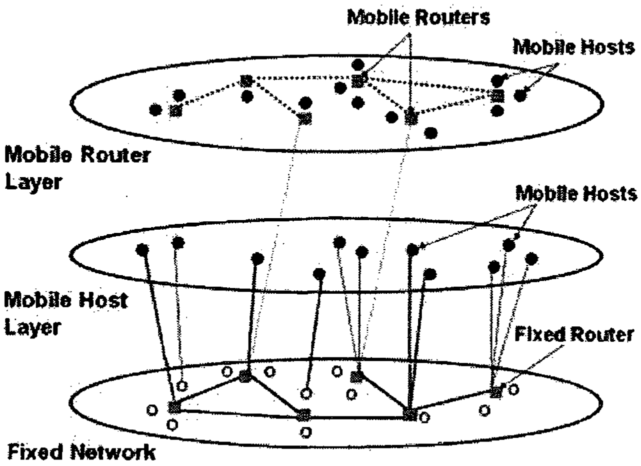


Figure 2.5: Architecture of the mobile Internet.

Authors in [43] described the mobile Internet as the coexistence of fixed and mobile infrastructures. The proposed architecture has two layers, the mobile host layer could be supported by Mobile IP or dynamic host configuration protocol (DHCP). The mobile router layer will likely be composed of separate autonomous systems of mobile routers or even contain satellite-based and aerial nodes, which may serve better mobile users requirements (figure 2.5)[2]. Mobile hosts in the first layer are one hop away from the fixed routers and are attached to them via either wired or wireless connections. The fixed routers act as gateways to the Internet and could even be Mobile IP foreign agents, which allow interaction with the fixed Internet through Mobile IP.

[2] Taken from [44]

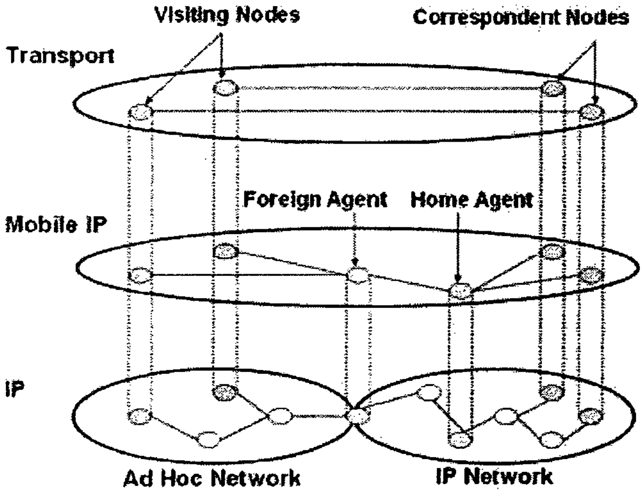


Figure 2.6: MIPMANET architecture.

Mobile IP for Mobile Ad Hoc Networks (MIMPANET) [45] enables visiting nodes to get wireless access, as shown in figure 2.6[3]. MIPMANET uses Mobile IP with foreign agent care-of address and reverse tunneling, and exploits the mobility services of Mobile IP. MIPMANET combines Mobile IP protocol, which guarantees location-independent routing, and AODV routing protocol [14], which is reactive in nature. When a visiting node wishes to communicate with a correspondent node on the Internet, it should tunnel its packet to the Mobile IP foreign agent it is currently registered with, which will de-tunnel it and forward it to the Internet. It is clear that Mobile IP foreign agents act as default routers for the visiting node. The use of tunneling helps implement the notion of default router within the MANET. Mobile IP foreign agents advertise their presence by broadcasting their agent advertisements. A visiting node will be able to select a foreign agent based on the hop count metric. According to the MIPMANET cell switching (MMCS) algorithm, a registered visiting node should switch to a new foreign agent if for two consecutive agent advertisements, it is at least two hops closer to this foreign agent than to its current one. Any message sent by a correspondent node to a visiting node will be

[3] Taken from [44]

received by the Mobile IP foreign agent currently serving the visiting node. The foreign agent will forward the message to the visiting node.

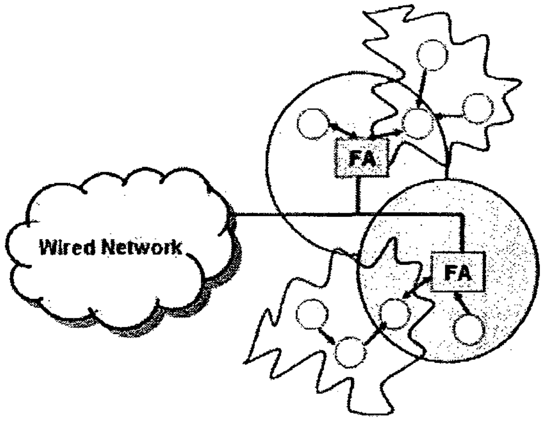


Figure 2.7: Internet connectivity to MANETs using foreign agents.

Authors in [46] proposed an approach using AODV routing protocol and Mobile IP to provide MANET nodes with Internet connectivity (see figure 2.7)[4]. Furthermore, they suggested a simple scheme allowing mobile nodes to obtain co-located care-of addresses when care-of addresses are not available. Co-located care-of address assignment requires at least one gateway be located between a MANET and the Internet to advertise routable network prefixes on the underlying network. Mobile nodes should also run a duplication address detection to guarantee uniqueness of their selected IP addresses. When foreign agents exist, Mobile IP protocol is used to provide mobile nodes with care-of addresses, while AODV is exploited for route discovery and maintenance within MANET. Mobile IP foreign agents advertise their presence via periodical agent advertisement, which are broadcast within a MANET. The interested mobile nodes unicast their request registration to the selected foreign agent using available fresh routes. Then, mobile nodes can start their Internet access session and communicate with the wired Internet through their selected Mobile IP foreign agents. Alternatively, a mobile node can discover existing foreign

[4] Taken from [44]

agents by proactively sending a route request targeting all mobility agents multicast group address 224.0.0.11. In order to find whether a particular destination is within a MANET or on the Internet, a mobile node broadcasts a route request within a MANET. If the source node receives a route reply from a mobile node, it concludes that the destination is located within a MANET. Otherwise, the destination is on the Internet if the source node receives a special route reply from a foreign agent. They use a modified version of the MMCS algorithm, where a mobile node can perform handoff only if it has not heard from its current foreign agent for more than one beacon interval or its route to it has become invalid. Packets from MANET nodes to the Internet are forwarded to foreign agents using standard IP routing, i.e., without tunneling.

2.5.2 Three-tier Architecture

In [47], authors are trying to address the problem of high mobility of mobile nodes and transparent migration of mobile nodes between gateways, by suggesting a three-tier architecture using mobile gateways to provide an efficient interface between *ad hoc* networks and the Internet. Another layer of mobile gateways is introduced to guarantee continuous, wireless Internet access to MANET nodes. These mobile gateways are supposed to be a part of a MANET and have permanent home addresses.

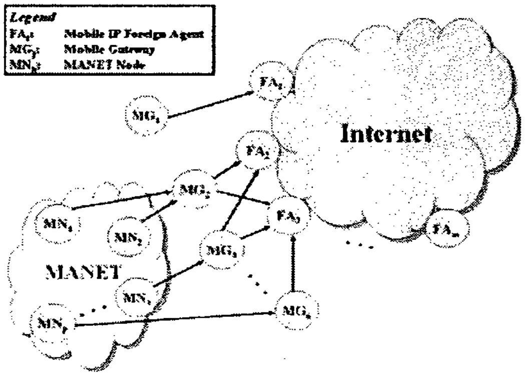


Figure 2.8: Three-tier architecture using mobile gateways.

The proposed three-tier architecture for connecting MANETs to the Internet is given in Figure 2.8[5]. The three layers are described below starting from the inner layer through the outer layer. The first layer contains Mobile IP foreign agents; the second layer includes mobile gateways and mobile hosts, which are one-hop away from Mobile IP foreign agents; the third layer has all MANET nodes and visiting mobile hosts that are at least one-hop away from mobile gateways. From now on, MANET nodes or visiting mobile hosts will simply be designated as MANET nodes, unless stated otherwise. Mobile gateways are designed in a way to provide Internet connectivity to MANET nodes using both Mobile IP protocol when they communicate with the Internet and DSDV protocol when they interact with MANET. In addition, mobile gateways guarantee access transparency of foreign agents by MANET nodes. In other words, MANET nodes do not recognize which foreign agents are indirectly providing them with Internet connectivity. However, mobile gateways will have to select appropriate foreign agents, which will offer Internet access to MANET nodes in a transparent manner. This selection is based on the load of these foreign agents and the distance between them and mobile gateways.

Authors then list the advantages of mobile gateways as follows:

- The presence of a layer of mobile gateways is useful to decrease the load that will be placed on the Mobile IP foreign agents if they were to take care of the registration of MANET nodes desiring Internet connectivity with them.

- The high movement speed of MANET nodes will increase the frequency of disconnections from the wireless Internet and degrade the performance of the hybrid, wireless network. Thus, the presence of a layer of mobile gateways in addition to the fixed Mobile IP foreign agents cancels out MANET nodes high speed, reduces their number of disconnections, and maintains continuous wireless Internet access.

[5] Taken from [44]

- A wide coverage area of Mobile IP foreign agents is a desirable feature. Mobile gateways can move at the border of these foreign agents and allow MANET nodes to register with them. This will widen the coverage area of these Mobile IP foreign agents.

- In many networking problems, it is necessary to evenly distribute the load on the available servers. MANET nodes are only aware of the presence of mobile gateways. Thus, mobile gateways can switch from one Mobile foreign agent to another transparently and independently of MANET nodes in order to meet some service requirements. Mobile gateways can switch to the least loaded Mobile IP foreign agent, which will balance the load on these foreign agents after the hybrid network has reached certain stability conditions. Similarly, MANET nodes can select the least loaded mobile gateway and register with it. This will create a balanced load on these mobile gateways. This transparent migration should not affect the interaction between MANET nodes and their mobile gateways, and that between mobile gateways and their Mobile IP foreign agents.

- Any wireless Internet access provided to MANET nodes should go through mobile gateways. These gateways constitute a barrier to authenticate any node desiring Internet access and prevent an intruder MANET node from having Internet connectivity.

- MANET nodes can move randomly and at unpredictable times. Thus, a MANET can be split into a set of sub-MANETs, where interactions between MANET nodes belonging to two different sub-MANETs cannot occur anymore. Mobile gateways are more powerful than ordinary MANET nodes in terms of coverage range and functionality, and can make this kind of communication happen.

- Mobile gateways yield more flexible, hybrid wireless networks and efficient Internet connectivity. This helps meet the quality of service (QoS) of the multi-hop wireless Internet access, measured in terms of responsiveness and high data delivery ratio.

2.6 Conclusion

In this chapter we introduced the ad hoc networks and different challenges. However, as we discussed earlier ad hoc approaches can not be used in VANET scenarios, because of the high mobility, scale and different behavior of the networks. Internet access approaches introduced here are not appropriate to be used in VANET scenarios. For two-tier approaches, they are not able to support the large number of vehicles on the road and also they are not designed to handle the high speed of the mobile nodes as in VANET. The three-tier architecture on the other hand is scalable and can support large number of the nodes on the road, however it is based on mobile gateways which is different from our case where we assumed that gateways are stationary.

Supporting mobile gateways in VANET is also possible. Some vehicles can be connected to the Internet using 3G networks (e.g *Universal Mobile Telecommunications System (UMTS)*) and share it with other vehicles. However, the cost efficient approach to provide the high speed Internet on the road is by implementing fixed base stations beside the roads, and through different Internet service providers. In the next chapter we are going to talk about Vehicular Ad hoc Networks and in section 3.6 we discuss the existing approaches to connect such networks to the Internet.

Chapter 3

Background and Related Work: Vehicular Ad-hoc NETworks (VANET)

For an understanding of the requirements and problems of Internet access in VANET, it is necessary to understand the overall concept of VANET. We first start by explaining what is VANET, then we discuss various VANET application, information dissemination, routing, security and Internet access in VANET.

In future vehicular networks, each vehicle is equipped with on-board sensors (rain sensor, tire pressure control, etc.), wireless communication system, positioning system, digital road map, a processing unit and storage devices. A vehicle uses its sensors to collect some data about the environment and the vehicle itself. It uses the wireless communication system to communicate with other vehicles and gather extra data about the traffic and environment. It also uses the positioning system and a digital road map to obtain the vehicle's geographical location and to match this location on the map, in addition to using this information to inform other vehicles about its location. Processor and storage devices are used to analyze and store the received data, either by sensor or other vehicles. This equipments are necessary for different VANET applications.

3.1 Outline

In this chapter we overview the vehicular networks in general and discuss the different challenges in such networks. VANET applications will be discussed in section 3.2. Section 3.3 and 3.4 discuss different protocols for information dissemination and routing in VANET. Security vulnerabilities and challenges will be covered in section 3.5. In 3.6 we will talk about existing approaches for connecting vehicular networks to the Internet and discuss their strengthes and weaknesses. Finally section 3.7 concludes this chapter.

3.2 Applications

Vehicular networks aim to provide safety for the vehicles on the road and controls the traffic by providing on time critical information for both the vehicle and the driver. Other than the safety applications, vehicular networks can be used to provide information to the driver and the passengers of each vehicle or it can be used to entertain them. Therefore, we classify the applications of vehicular networks into three categories: Safety & Driver assistance applications, traffic control applications and infotainment (information and entertainment). We will discuss each category in detail shortly. [48]

3.2.1 Safety and Driver-assistance Applications

The applications that fit into this category are trying to make the roads secure and safe by spreading the alarm messages or information before the driver reaches a point

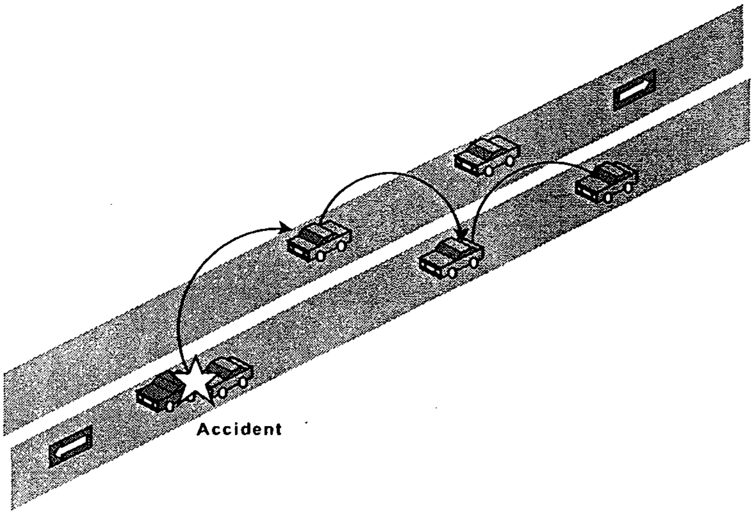


Figure 3.1: Spreading the alarm messages by vehicles on the opposite direction. This will inform other vehicles to slow down or change their lanes.

beyond which he has no time to prevent the accident, e.g., road condition data can be exchanged among vehicles. For instance, in the case of an accident, information of the accident can be disseminated through the vehicle network by both the vehicles that move in the same direction or in the opposite direction to inform the vehicles that might run into the accident. Figure 3.1 illustrates a scenario in which, the information about the accident is spread in the network by the vehicles that are moving in the opposite direction of the movement.

Assisting the driver by using signages, e.g., traffic signal, stop sign, rail crossing violation warning, etc., can help the driver to notice the different signs before he gets to the point. Assisting the driver at intersections by giving an intersection collision warning or help the driver while he decides to turn left, can reduce the number of accidents or totally eliminate them. Vehicular networks can also be used to inform the driver about the road conditions, such as obstacles on the road, work zone warning, black ice, etc.

Informing the driver of potentially dangerous situations is another application for VANET. Among these applications are blind spot warnings, lane change warning and wrong way driver warning. In addition, if an accident happens they can spread crash/breakdown warning messages, inform authorities to take proper decisions and record the relevant data in the integrated Event Data Recorder (EDR) in the vehicle for further references.

All the applications in this category require position awareness of the vehicles, addressing of vehicles on the basis of their current position, short transmission delay and high reliability of data exchange. The hit rate needed to realize these services is low. These applications provide an excellent example of the need for exchange of data that is of local relevance. [48]

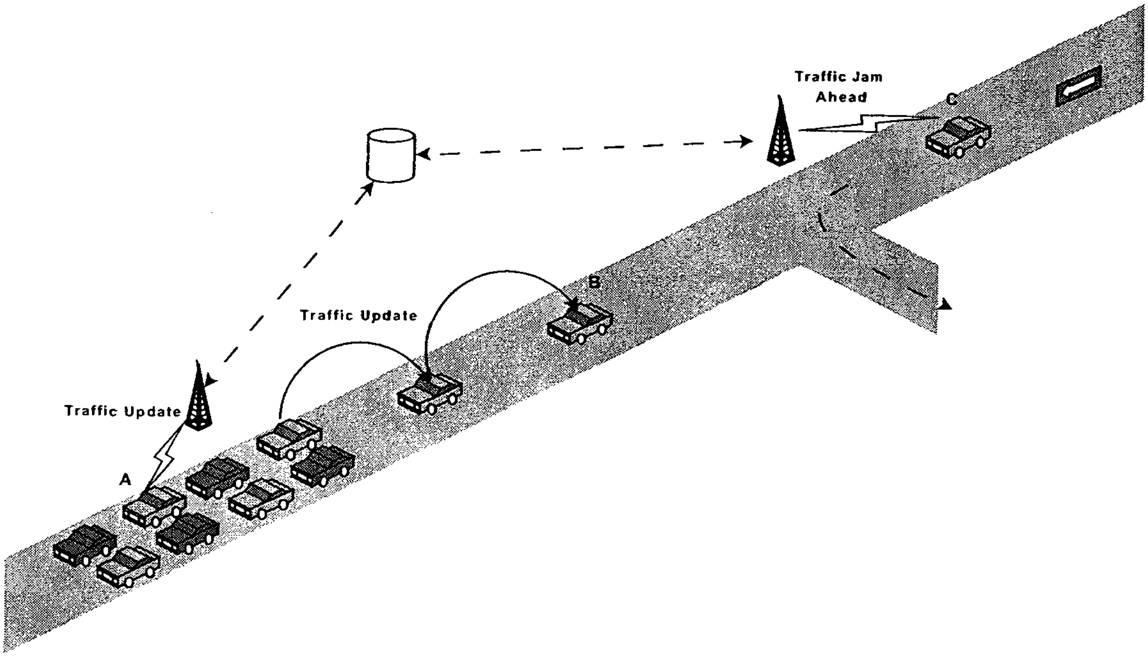


Figure 3.2: Traffic information is broadcast in the network by vehicles or infrastructure units.

3.2.2 Traffic Control Applications

Currently centralized solutions are used to control the traffic flow. Specific centers collect and combine the data from vehicles and broadcast the result back to the service users. However, such a service can be realized without any centralized information processing in a local inter-vehicle communication system which exploits position-awareness for data distribution, thus avoiding the use of service centers and expensive transmissions via cellular radio systems. Relevant traffic information can be easily disseminated in the opposite direction of the traffic flow, and inform the following cars about the traffic conditions ahead. Traffic information can either be spread in the network by vehicles or roadside infrastructure units.

Figure 3.2 shows a simple scenario with a traffic jam in the highway; vehicle **B** and **C** are not part of the congestion yet. Vehicle B will receive the information via broadcast messages from other vehicles ahead. Vehicle **A** communicates with the closest roadside unit and updates it about the traffic jam, the unit then sends the information to a central unit. Other neighboring roadside units receive these updates and immediately update the vehicles nearby and inform them about the traffic situation ahead. Vehicle **C** will receive this information from the closest roadside unit before it joins the congestion, and takes the first exit to skip the traffic congestion ahead.

Assuming that vehicles are equipped with digital maps or GPS, and thus aware of the route to the destination, they can send queries to other vehicles in the route about the traffic flow or weather/road conditions. If a traffic jam is detected, alternative routes can be calculated in no time, in this way the driver can avoid the highly packed roads and take a faster route to the destination and save a lot of time and money. The requirements placed on the radio communication system are low position accuracy, low data transmission reliability, and medium priority. However, it is expected that data transmission will occur periodically, so that periodical time slots are to be reserved by the channel access scheme [48].

3.2.3 Infotainment

Other than helping the driver, providing safety and traffic control which are the main reason for vehicular networks to appear, vehicular networks can be used to entertain the driver and passengers. Services such as Internet access, mobile advertising, inter-vehicle games, distributed games and toll collection can be provided using vehicular networks. We will talk about the different approaches to provide the high speed Internet access on the road later.

3.3 Information Dissemination

The main goal of VANET is to provide safety on the road and improve the traffic control by spreading safety messages and traffic messages into the network. However, using IP broadcasts are not efficient as they can flood the network and consume most of the network bandwidth. Beside that, many features of vehicular network such as the scale, high speed of the vehicles, short-lived communication links and changing of the information based on the position and time is among the challenges which makes it hard to design a protocol to disseminate the information in a timely manner. Safety applications also has critical latency requirements. We briefly review the available broadcast mechanisms and introduce two dissemination protocols.

Broadcasts are usually used in different networks to disseminate the information in the network. However, as mentioned earlier, broadcasts consume most of the bandwidth. These are some different approaches for broadcasting in VANET:

- **Flooding.** The simplest way to disseminate information is to flood the message into the network. However, this will lead into contention, collision and message redundancy which is known as *the broadcast storm* [49]). Besides, flooding can not keep the message in a certain area and the message can be broadcast over and over again along a long road, while it is not necessary. Also, the message may not be broadcast at all if there is no neighboring node around, which is not desirable in case of spreading the safety messages.

- **Deterministic Broadcast.** This type of broadcast guarantees the packet delivery to all the nodes in the network. Guaranteed packet delivery is not efficient in VANET due to the large scale of the network and high speed of the vehicles, plus that the delivery of the information to all the vehicles is not required in VANET.

- **Probabilistic Broadcast.** Assure the delivery of the message by a certain probability. In these schemes, a node rebroadcasts a message with a certain probability. They multicast the packet in the network and by using the negative acknowledgments control the success of the transmission. Although these protocols consume less bandwidth than deterministic protocols, they still have a very high overhead for disseminating the information. There is still no support for dissemination areas and disseminate the message within the whole network.

- **Location-Based Broadcast.** These methods use the location information of a node to decide whether this node should broadcast the message or not. These protocols can be used to disseminate the information in a certain area, and since not all the nodes are broadcasting it will reduce the amount of the overhead and is scalable. These protocols are the most suitable protocol among the broadcast protocols for VANET.

Knowing different broadcasting approaches in VANET, we only introduce two disseminating protocols for disseminating safety information:

Vehicle-to-vehicle location-based broadcast (LBB) [50] is addressing the safety communication on highways. In this protocol, source nodes assign a life-time to each message before broadcasting the message. Using this life-time, each node will broadcast the message when it receives the message within the life-time of the message, otherwise the message will be dropped. Moreover, vehicles rebroadcast the message based on a random decision to avoid collisions. However, collisions may still occur if two or more vehicles broadcast at the same time. This protocol suffers from the lack of a good algorithm to assign a proper life-time to each message, since different messages have different requirements.

Optimized dissemination of alarm messages in vehicular ad hoc networks (ODAM) [51] restricts the rebroadcast to certain vehicles, and messages are only broadcast in some specific areas called risk zones. This protocol suggests a new approach to rebroadcast the messages based on the contention based forwarding (CBF) [13]. A timer will be set based on the distance that each vehicle has to the source node, and the furthest vehicle from the source node will set the shortest timer. When this timer expires, if the node has not received any other rebroadcast messages from other nodes, it will rebroadcast the message in the network and suppress other nodes. The coordination of the risk zone will be included in the broadcast message. While receiving a message, each node checks its location information against what is included in the message to see if it is inside the risk zone or not. If so, it will set a timer, otherwise it will not forward the message any further.

3.4 Routing in VANET

Designing a routing protocol for vehicular networks faces many challenges, among which are the high speed of the vehicles, fast topology changes and the number of vehicles on the road. On the other hand, nodes in VANET have enough computing, power and storage resources and vehicles usually move in the boundary of roads and somehow their behavior is predictable. MANET routing protocols can be used in VANET scenarios, however most of these protocols are not scalable and also can not handle the high speed of the vehicles and the fast topology changes in VANET. First we argue about the pros and cons of using different MANET routing protocols in VANET, then some routing protocols designed for VANET will be presented.

Using proactive routing protocols in VANET scenarios have some drawbacks. First of all, in these protocols all the nodes or part of them are using IP broadcast to update the other nodes about their existence, and IP broadcasts in a large network such as VANET can easily flood the network. Next, considering the large number of the nodes in the network, control messages overhead will consume most of the bandwidth in scenarios where there are many vehicles available. These protocols do not have any latency in route discovery, and if a node wants to send a packet, it can send it immediately.

Reactive routing protocols can not be used in VANET scenarios and they also have some drawbacks. Since discovering routes in these approaches is time consuming, in a network such as VANET where the links are not stable for a long time, this can cause some problems and cancel the QoS features required by some applications. These protocols however do not flood the network and the overhead of the route discovery is reasonable. In [52] authors have compared the performance of some topology-based routing protocols in city traffic scenarios.

As explained in section 2.3.2, position-based routing approaches do not require routing tables or storing of routes. But instead, they use the position information of nodes to deliver the packets to the destination. These protocols seem to be a good option to be used by VANET. Vehicles in VANET are using GPS and are aware of their positions, and this solves the problem of location awareness that is required by position based protocols. Besides, position-based protocols alleviate the problems of scalability and control message overhead and has been shown to have higher delivery rates than topology-based routing approaches. In [53] authors compared DSR with GPSR in VANET and concluded that position-based routing is more promising than topology based protocols in VANET scenarios.

Geographic forwarding, as in position-based protocols, works well in high density networks but poorly when there are frequent topology holes due to building and road structures. Generic position-based routing schemes do not take into account the impact of fixed environment conditions which will change transmission range, causing routing loops and wrong direction routing. Recovery methods are often used to circumvent the topology hole but since most of the algorithms are stateless, each packet nearing a topology hole will have to go through the same recovery process. This becomes inefficient when the topology hole is permanent (e.g., physical road constraints).

Geographical Source Routing (GSR) [54] uses position-based routing supported by map of the city for more correlated routing to the physical topology of city environments. Similarly, *Spatially-Aware Routing (SAR)* [55] uses a spatial environment model to proactively avoid permanent topology holes. Position-based routing protocol predicts and avoids route recovery caused by permanent network voids. SAR relies upon the extraction of a static street map from an external service such as GIS (Geographic Information Systems) to construct a "Spatial model" for routing. However, there is no guarantee that the forwarding node can find a suitable neighbor along the given intermediate geographic locations. To recover from this situation, a node can suspend the packet in the buffer for a period of time while waiting for a suitable neighbor. In comparison studies [55], SAR handles topology holes better than generic greedy forwarding schemes [56].

Beacon-based routing scheme may not provide accurate information of neighbors and can incur large overhead in highly mobile cases. As explained in section 2.3.2, *Contention-Based Forwarding (CBF)* [13], is a greedy forwarding scheme which does not utilize position beacons to determine next-hop node. In [57] CBF is shown to increase packet delivery ratios compared to beacon-based routing in street scenarios.

In addition, nodes do not store neighbor information and there is no increase in bandwidth (for beacons) as mobility increases.

Besides the MANET routing protocols, some protocols have been designed to be used particulary in vehicular Networks. **Connectivity-Aware Routing (CAR)** [58] is a VANET position-based routing protocol designed for city and/or highway environment. A distinguishing property of CAR is the ability to not only locate positions of destinations but also to find connected paths between source and destination pairs. These paths are auto-adjusted on the fly, without a new discovery process. "Guards" help to track the current position of a destination, even if it traveled a substantial distance from its initially known location.

In CAR all the nodes send HELLO beacons including the information about their moving directions and speeds. All nodes cache this information when they receive the HELLO message. The recorded information expires after two HELLO intervals, or when the estimated positions of the current node and the neighbor become separated by more than 80% of the average coverage range (whatever is smaller). The CAR protocol uses an adaptive beaconing mechanism where the beaconing interval is changed according to the number of the registered nearby neighbors. The fewer neighbors there are, the more frequent is a node's HELLO beaconing.

To capture key components of a path, CAR introduces the concept of a guard. There are two types of guards: *standing guards* and *traveling guards.* A node with a guard can filter or redirect packets or adds information to a packet that will eventually deliver this information to the packet's destination. To find a destination and a path to it, CAR uses *Preferred Group Broadcasting (PGB)* in data dissemination mode. PGB optimizes broadcasts specifically for VANETs, it reduces control messages overhead by eliminating redundant transmissions. CAR explains that a node adds an anchor to a broadcast packet if the direction of the node's velocity vector is different (non-parallel) from the Previous forwarder velocity vector field. An anchor contains two anchor points - the coordinates of the current node and the coordinates of the previous forwarder as well as their velocity vectors.

The CAR protocol extents *Advanced Greedy Forwarding (AGF)* [59] to work with anchor points. Instead of forwarding a data packet to a neighbor that is geographically closer to the destination, a neighbor closest to the next anchor point is chosen. To avoid multiple attempts to gradually get closer to the next anchor point, each forwarding node checks if its position and the position of the next anchor point is separated by less than half the node's coverage range. If so, then this anchor point is marked and the next one is chosen as target. The process continues until the packet reaches its destination. CAR uses the guards for path maintenance, and it also introduces a scheme for routing error recovery.

GVGrid [60] is a QoS routing protocol for VANET which constructs a route on demand from a source (a fixed node or a base station) to vehicles that reside in or drive through a specified geographic region. The goal of GVGrid is to maintain a high quality route, i.e., a robust route for the vehicles' movement. Such a route can be used for high quality communication and data transmission between roadsides and vehicles. or between vehicles.

GVGrid uses digital map and position information of each vehicle to discover a network route which is expected to provide the best stability. It uses the characteristics of the movement and the driving route to determine the stability. It also offers a restore policy which restores the broken network routes while the vehicle is moving towards the destination. This protocol divides the map into grids, and each vehicle should know the destination to find the destination grid and send the RREQ messages toward that grid.

Movement Prediction-based Routing (MOPR) [61] is a VANET routing protocol which improves the routing process by selecting the most stable route in

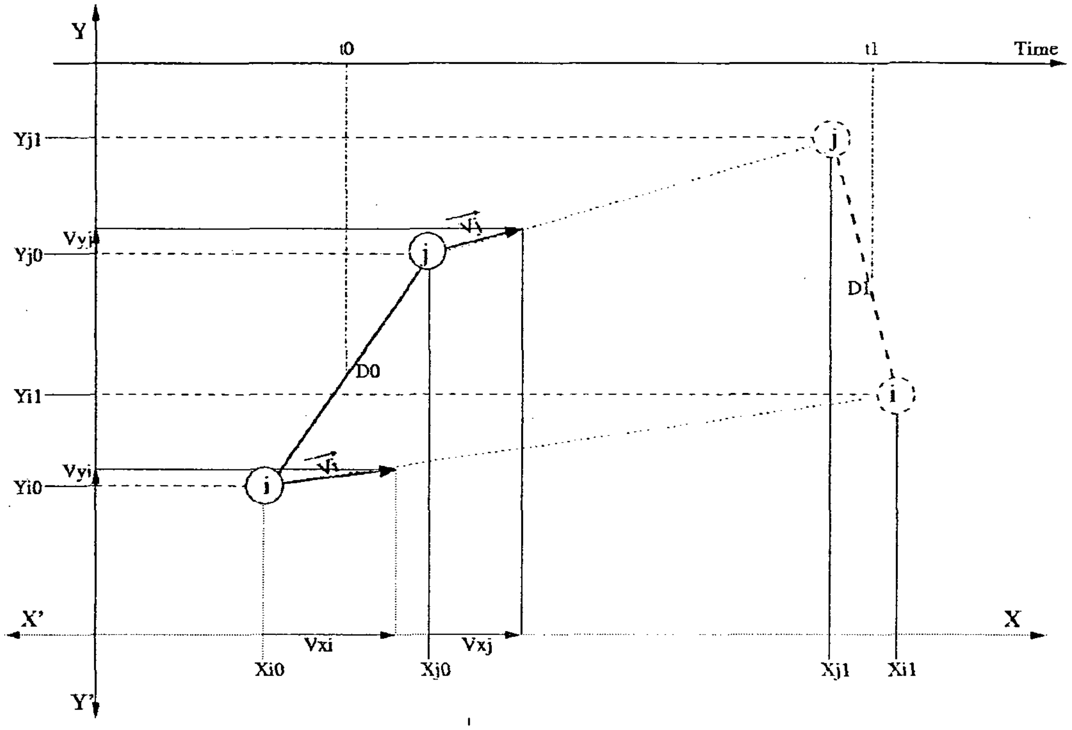


Figure 3.3: MOPR link life-time estimation.

terms of life-time with respect to the movement of vehicles. MOPR, based on vehicles' movement information, guarantees the selection of the best next hop for data forwarding.

In this protocol each vehicle estimates the Link Stability (LS) for each neighbor. The LS is a relation between the link communication life-time and a constant value (say: σ) which represents in general cases the routing route validity time, and it depends on the used routing protocol. Figure 3.3 shows how link life-times are estimated based on neighbors' movement information. The life-time of the link (i, j) ($Lifetime[i, j]$) corresponds to the estimated time $\Delta\ t = t_1 t_0$ with t_1 is the time when D_1 becomes equal or bigger than the communication range R (i.e., the time when j goes out of the communication rage of i). D_1 and $\Delta\ t$ are estimated using the initial positions of i and j ((X_{i0}, Y_{i0}) and (X_{j0}, Y_{j0}) and their initial speeds $\vec{V_i}$

and $\vec{V_j}$ respectively).

$$D_1^2 = \left((X_{i0} + V_{x_i}\Delta\ t) - (X_{j0} + V_{x_j}\Delta\ t)\right)^2 + ((Y_{i0} + V_{y_i}\Delta\ t) - (Y_{j0} + V_{y_j}\Delta\ t))^2$$

$$D_1^2 = A\Delta\ t^2 + B\Delta\ t + C$$

Where:

$$\begin{aligned} A &= (V_{x_i} - V_{x_j})^2 + (V_{y_i} - V_{y_j})^2 \\ B &= 2[(X_{i0} - X_{j0})(V_{x_i} - V_{x_j}) + (X_{i0} - Y_{j0})(V_{y_i} - V_{y_j})] \\ C &= (X_{i0} - X_{j0})^2 + (Y_{i0} - Y_{j0})^2 \end{aligned}$$

By solving the equation $A\Delta\ t^2 + B\Delta\ t + CR^2 = 0$ we can easily find the $\Delta\ t$ which corresponds to the $LifeTime[i,j]$ we are looking for. Now, LS is calculated as follows:

$$LS[i,j] = \frac{LifeTime[i,j]}{\sigma}$$

where $LS[i,j] = 1$ when $LifeTime[i,j] \geq 0$.

After computing the LS, MOPR selects the next forwarding hop according to the calculated LS. The link with the highest LS (corresponding to the most stable neighboring link) will be selected to forward the packets through the connected neighbor to the link. The authors then apply MOPR on GPSR [15] and create a new protocol called MOPR-GPSR. Authors have applied MOPR in a different way. When a vehicle wants to send or forward data, it first estimates the future geographic location after a duration time T in seconds for each neighbor. Then, it selects as next hop the closest neighbor to the destination which does not have a future location out of its communication rage after the time T. Other than this position based approach, in [62] authors introduce MOPR-OLSR which tries to improve this proactive routing protocol to be used in vehicular networks.

3.5 Security

Implementation of vehicular networks, will be a great improvement to the safety of the roads. However, using these networks without taking the security into account can be more fatal than using non-equipped vehicles. In designing each protocol for vehicular networks, one must make sure that the protocol is fully secure and resilient to attacks. Here we will investigate different vulnerabilities in vehicular networks, and challenges that must take into consideration while designing a protocol for vehicular networks [63].

3.5.1 Vulnerabilities

Attackers can use a wireless device that runs a rogue version of vehicular communication protocol stack to pose some threats. Here we will explore different vulnerabilities threats for vehicular networks.

Jamming – Deliberately generating interfering transmissions that prevent communication within the reception range of a wireless device is called jamming. As the network coverage area (e.g., along a highway) can be well-defined, at least locally, jamming is a low-effort exploit opportunity. As figure 3.4 shows, the vehicular network is partitioned by a jammer. This can be done easily without using any cryptographic mechanism and using a limited transmission power.

Forgery – An attacker can easily sends incorrect information, or delay the reception of critical information. This wrong or delayed information can be the reason for an accident or a traffic jam. Figure 3.5 illustrates how fast the vehicular network can get contaminated with false information where a single attacker forges and transmits

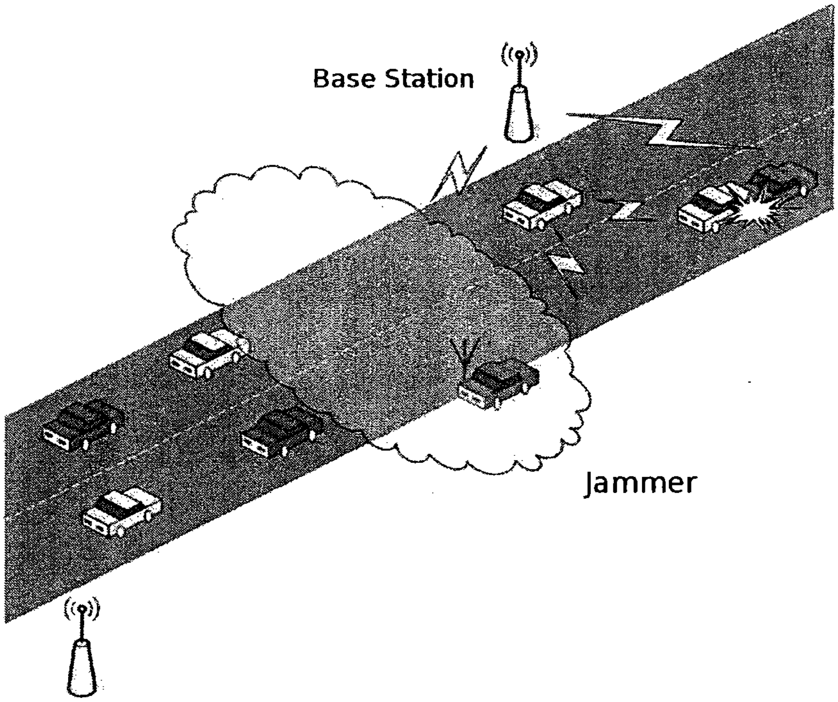


Figure 3.4: Spectrum jamming.

false hazard warnings (e.g., traffic jam is ahead), which are taken up by all vehicles in both traffic streams.

In-transit Traffic Tampering – Since in VANET information is spreading using multiple hops, any intermediate node can disrupt the communications of other nodes. It can drop a message, corrupt it or intentionally change the content of the message. In this way, the reception of valuable or even critical traffic notifications or safety messages can be manipulated. Replaying old messages is another issue (e.g., to illegitimately obtain services such as traversing a toll check point). This kind of attack can be stronger and more effective than forgery.

Impersonation – Impersonation is the act of faking the identity of a vehicle or base station. Mostly the content of the message (e.g., hazard warning) and the attributes of the message are more important than the source of the message.However, an impersonator can be a threat: consider, for example, an attacker masquerading

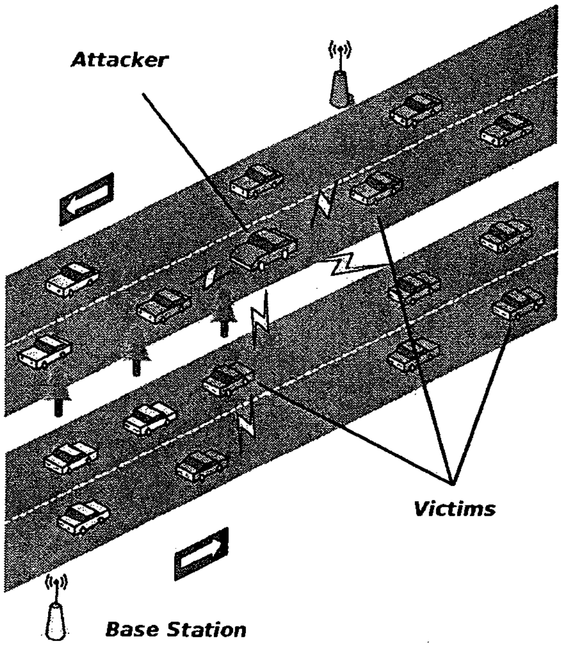


Figure 3.5: Message forgery.

as an emergency vehicle to mislead other vehicles to slow down and yield; or an adversary impersonating roadside units, spoofing service advertisements or safety messages.

Privacy Violation – Since in vehicular networks, the private information of vehicles are exchanged in the network, the collection of this information from the overhead of vehicular communications becomes easy. Many services in vehicular networks require registrations of the driver information in order to provide the service (e.g., over-the-air registration with local highway authorities). In these occasions, an attacker could precisely identify the originating node as well as the drivers' actions and preferences. This information can be used to track a vehicle or spy on the driver's actions and behaviors while on the road.

On-board Tampering – An attacker also can easily change the wiring of a sensor or replace or by-pass the real time clock rather than hacking the communication protocols. For example, if someone had an accident and left the scene, the data will be available on the hardware and it starts to send out the information to all the vehicles around. One can change the hardware in order to not save the accident related data or informing other vehicles in this way. So the hardware used in vehicular communication should be tamper-proof as well.

3.5.2 Challenges

Based on vulnerabilities that were mentioned earlier, the task of securing vehicular networks becomes very challenging and dynamic. Here we list the challenges in this field:

Network Volatility – Due to the high mobility of vehicles on the road, the duration of each connection from a vehicle to another vehicle or from a vehicle to a road infrastructure unit is very short. Therefore, password-based establishment of secure channels, gradual development of trust by enlarging a circle of trusted acquaintances, or secure communication only with a handful of endpoints may be impractical for securing VANET.

Liability vs. Privacy – The accountability and, eventually, liability of the vehicles and their drivers are required. It means that at the same time, the identity and information of the driver should stay private and obtaining hard-to-refute data that can assist legal investigations (e.g., in the case of accidents) should be possible.

Delay-Sensitive Applications – Many of the envisioned safety and driver-assistance applications pose strict deadlines for message delivery or are time-sensitive. These constraints must be taken into account and impose a low processing and messaging overhead. These protocols must be lightweight and at the same time be resistant to clogging denial-of-service attacks.

Network Scale – Large number of vehicles (billions of vehicles around the world) plus multitude of authorities governing transportation systems makes it difficult to provide cryptographic keys for vehicles.

Heterogeneity – The heterogeneity in VANET technologies and the supported applications are additional challenges, especially taking into account the gradual deployment. For example, GPS signaling can be spoofed, then the correctness of node coordinates and time accuracy cannot be assumed.

Securing vehicular networks is a very challenging task, as explained earlier. However, this part is still an open subject and requires the attention from academy and industry to become practical. There are not many works addressing the subject of vehicular network security. Gerlach [64] describes the security concepts for vehicular networks. Hubaux et al. [65] take a different perspective of VANET security and focus on privacy and secure positioning issues. They point out the importance of the trade-off between liability and anonymity and also introduce Electronic License Plates (ELPs), unique electronic identities for vehicles. Parno and Perrig [66] discuss the challenges, adversary types, and some attacks encountered in vehicular networks; they also describe several security mechanisms that can be useful in securing these networks. Raya and Hubaux [67] describe a full security and privacy framework for VANETs with primary simulation evaluations of the security overhead. El Zarki et al. [68] describe an infrastructure for VANET and briefly mention some related security issues and possible solutions.

3.6 Internet Access in Vehicular Ad hoc NETworks

Providing high speed Internet access for moving vehicles on the road is challenging, due to the high speed of the vehicels and fast topology changes in vehicular networks. Discovering gateways, establishing a connection to them and handing over the connection to the next gateway are challenges that should be taken into consideration before designing a protocol for this purpose. Large number of vehicles on the road, on the other hand, makes it even harder. Broadcast should be done wisely in order to prevent flooding the network, providing unique IP addresses requires using IPv6 address space. Besides, each vehicle should have a unique IP address and aside from its location, it should be reachable using that IP address. These are all different problems that must be solved before designing a protocol that integrates the VANET network into the Internet. In this part, we discuss existing protocols that aim to provide Internet access for vehicles on the road.

The Fleetnet Project [69] has accomplished a lot of work on Inter-Vehicular Communication (IVC), and investigated the VANET Internet Integration through stationary roadside gateways [70, 71]. It uses a modified version of Mobile IPv6 to handle the mobility, proposed a service discovery protocol for gateway discovery and also uses location based routing protocols to route packets. A new communication architecture called MOCCA (MObile CommuniCation Architecture) was developed for efficient Internet Integration for future vehicular ad hoc networks.

In [70] authors introduce new ways for gateway discovery in future vehicular systems. They offer that Multi-hop vehicle-to-vehicle communications, future IVC systems will also comprise roadside installed gateways to the Internet. The Internet Gateways (IGWs) are on one hand integrated into the IVC system, on the other hand, they are connected to the Internet. The IGWs provide a cheap, however timely restricted access to the Internet for passing vehicles. However, those IGWs must be discovered by the vehicles in the ad hoc network. In contrast to conventional ad hoc networks formed by most other mobile devices (e.g., PDAs or laptops), vehicular ad hoc networks are highly mobile and dynamic, i.e., the network topology changes frequently. As a result, the availability of IGWs changes frequently, too, and several gateways might be available at the same time. Figure 3.6 illustrates the shape of

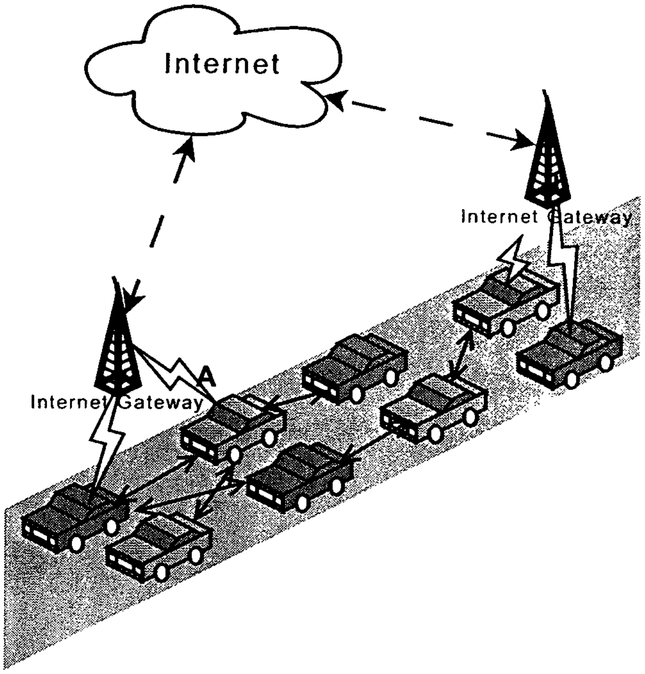


Figure 3.6: Fleetnet vehicular communication scenario.

the future vehicular communication scenario. Vehicles can either connect to the gateways directly or over multiple hops, gateway discovery should be extended over multiple hops. Vehicles have access to the Internet using these gateways.

DRIVE (DiscoveRy of Internet gateways from VEhicles) is the Fleetnet suggested protocol for service discovery in order to find the gateways and acquire the access to the Internet. In DRIVE gateways periodically advertise their services using geocast capabilities of vehicular systems. If a vehicle moves into the (virtual) transmission range of an IGW, it will find the service provided by the gateway and record it in its database. While a vehicle requires to use a service, it searches its database. If the search is successful, the in-vehicle functional unit will respond with the respective IGW. Otherwise, the user must assume that a gateway is currently not available. For gateway selection, authors introduced a fuzzy approach which selects the gateway based on some network parameters such as gateway available bandwidth, current number of clients and packet loss probability. However, they did not take fast mobility and movement parameters of the vehicles into account, which is important in order to prevent frequent fragmentation in the network.

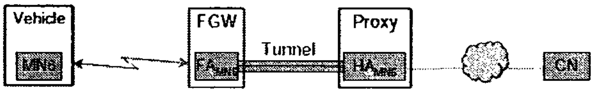


Figure 3.7: Mobile IP communication path.

In addition, in [71], MOCCA was introduced for mobility support. MOCCA assigns IPv6 internet address to the vehicles, and introduce a new approach for using the Mobile IP in vehicular networks. It combines a proxy-based communication architecture with a modified Mobile IP. The central element in MOCCA is a Proxy located at the transition point between the Internet and the FleetNet cloud. The Proxy may be hosted by an arbitrary Internet provider, e.g., under private operation. The FleetNet cloud not only covers the inter-vehicle networks but also the paths from the Internet gateways to the Proxy. Nodes can have a unique IPv6 address, and *Foreign Agents* are integrated into the road infrastructure units and they use a tunnel to access the proxy in which the *Home Agent* is integrated, and from there the request will be sent to the Internet (figure 3.7). This approach can fully support the mobility of the vehicles and provide them with unique IP addresses along the way. However, since the connections are short, the time required for registering the vehicle with the foreign agent must be considered as well.

In [72] authors suggest that **NEMO** (RFC 3964) can be used along with a VANET routing protocol to provide the Internet access for VANET. NEMO enables mobile nodes in ad hoc networks to attach to different points in the Internet. The protocol is an extension of Mobile IPv6 and allows session continuity for every node in the Mobile Network as the network moves. It also allows every node in the Mobile Network to be reachable while moving around. The Mobile Router, which connects the network to the Internet, runs the NEMO Basic Support protocol with its Home Agent. The protocol is designed so that network mobility is transparent to the nodes inside the Mobile Network. However, NEMO is designed for mobile networks with single-hop connectivity to a network infrastructure. The authors in [72] then investigate the possibility of combining NEMO with a VANET routing protocol. NEMO will provide the global reachability while VANET routing would handle the communication among vehicles and road-side infrastructure units.

Authors first argue about the economic, functional, performance and deployability requirements of vehicular networks. They mention that future vehicular networks should be cost efficient, support V2V and V2I communications, less overhead for the ad hoc part of the network and the mobility support should be able to cope with the fast topology changes and high speed of vehicles. Two approaches for NEMO in MANETs is introduced:

- **MANET-centeric Approach.** MANET-centric is a solution to apply NEMO in MANETs, in which multi-hop communication between a generic MANET node and infrastructure is achieved transparently by means of the MANET routing protocol, whereas NEMO runs on top of it. In this approach, the multi-hop path between a MANET node and an attachment point which is out of its direct wireless communication range relies only on a distributed routing protocol which is executed by all nodes participating in the MANET.

- **NEMO-centeric Approach.** NEMO-centric is a solution to apply NEMO in MANETs, in which multi-hop communication between a generic MANET node and infrastructure is achieved passing through at least one NEMO Mobile Router running on a different node. In this approach, the multi-hop path between a MANET node and an attachment point which is out of its direct radio range relies on one or more NEMO instances (Mobile Router) running on other nodes.

The authors then compare these two approaches based on the VANET requirements that they mentioned earlier. Finally, they propose that MANET-centeric approaches seems to be more appropriate to be used in VANET scenarios, for the following reasons:

- a more cost-efficient solution,
- easier direct V2V communication with intermittent infrastructure access,
- less complex support of geographic addressing,
- better routing performances, because of easier integration with reactive, VANET-specific ad hoc routing protocols.

However, there is no suggestion for how a unified protocol can combine NEMO with VANET, and no performance evaluation has been provided.

Controlled vehicular Internet access protocol with QoS (CVIA-QoS) [73] is a cross-layer solution for vehicular multihop networks spanning MAC and routing functions with infrastructure support. CVIA-QoS protocol uses admission control for soft-real time traffic to provide delay bounded throughput guarantees. To achieve this goal, fast and slow packet propagation methods are defined for real-time and best effort traffic, respectively.

CVIA assumes that gateways send periodic service announcements to indicate the availability of the service in their service area (messages can spread through multiple hop). In addition, they also assume that the up-link and the down-link packets are transmitted over two frequency separated channels. When a vehicle enters the service area of a gateway it registers itself with the gateway. The objective of the protocol is to *increase the end-to-end throughput while achieving fairness in bandwidth usage between road segments* for the best effort traffic. The CVIA protocol aims to solve two main problems of IEEE 802.11 protocol in multi-hopping along a highway: Low throughput and starvation of packets originating from vehicles far away from gateways.

CVIA divides the road into segments, which are fixed sections of each gateway service area. The time that a vehicle requires to traverse a segment is called a time slot. A vehicle is designated to each segment to control the traffic and called temporary router. In each time slot, temporary router which is responsible for the outbound traffic receives packets originating from other segments and local packets from its own segment. At the end of the time slot, all packets are moved out to the next segment together without contention.

However, in CVIA-QoS, one time slot is divided into two periods, namely high priority period (HPP) and low priority period (LPP). Unlike the CVIA protocol, packets admitted to HPP are delivered to the gateway in one time slot. Furthermore, an admission control mechanism is introduced where admission decisions are made by the gateways and executed by the temporary routers.

Authors in [74] study the feasibility of mobile gateways for vehicular ad-hoc networks, and also propose PRAODV and PRAODVM, two predictive based routing protocols which are variants of AODV. They first study the feasibility mobile gateways through simulation of the underlying connectivity characteristics for varying traffic and gateway densities. They evaluate the AODV routing protocol over different scenarios, and show that it performs well for the densities considered. However, since AODV can break frequently they introduce two prediction based routing protocols to support mobile gateways.

PRAODV retains most of the features of the AODV protocol. The main modification is in the RREP reply packet sent from the destination or intermediate nodes to the source. Whenever a node sends a reply, it includes its velocity and location information in the packet. Every subsequent node that receives this reply on route to the source of the request makes a link life-time prediction based on its own location and velocity and the values inside the reply packet from the node that sent it. It adds its predicted link value to the the reply packet replacing the old predicted value if its estimation of the life-time of link is smaller than any previous estimations of any link of the route. It also replaces the location and velocity information of the previous node with its own values before forwarding it towards the source. The basic idea is to have an estimation value which is the minimum of all links along the route. This is the predicted life-time of the route. A new request is sent out just before the end of this predicted life-time to construct a new route to the destination.

PRAODV-M uses the path which has the maximum predicted value among multiple route options as metric unlike AODV and PRAODV which use minimum hop count. The idea behind this is to minimize preemptive route creation by choosing the route which is expected to last the longest. How well the life-time of a route can be estimated plays a key role in the performance of this protocol.

To predict the life-time of a route, they argue that a route breaks when any one of the links break, and hence a route is only as strong as its weakest link. A link breaks when the two nodes on either side of it move out of the communication range, R, thus if two nodes are at a distance d_{ij} from each other, $R - |d_{ij}|$ represents the absolute distance the nodes have to separate additionally in order for the link to break. Thus if the two nodes have velocities V_i and V_j then the absolute difference in velocities is represented by $|V_{ij}|$. Thus the life-time of a link can be predicted as:

$$Pr.LinkLifeTime_{ij} = \frac{R - |d_{ij}|}{V_i - V_j}, V_i \neq V_j$$

For each route the route life-time will be the minimum calculated life-time of the links. The evaluation of their protocols in their paper shows that these protocols increase the delivery ratio, but on the other hand increases the overhead as well.

Authors in [75] evaluated the feasibility and the expected quality of VANETs operated with the routing protocol **DYMO (Dynamic MANET On-demand Routing Protocol)** [76] which tries to couple a MANET with the Internet. They suggested that cross-layer optimization of transport and routing protocols is required. Indeed, using DYMO or other ad hoc routing protocols present some drawbacks. These protocols do not typically select a route with sufficient life-time to maintain the longest possible duration of communication with a mobility agent. Another disadvantage relates to the handover mechanism of connections from one gateway to the next. From the use of Mobile IP, this mechanism is not sufficiently fast to manage hand-overs in VANET environment known as "Strong Mobility". Moreover, since more than one gateway may be available at the same time, the challenge becomes to discover gateways with the best quality of service (QoS) without wasting network resources. Here, quality of service encompasses notions such as path availability, stability, and small hand-over delays.

MMIP6 is a mobility management protocol for VANETs to integrate IPv6-based VANETs into the Internet [77]. It uses a proactive service discovery protocol for Foreign Agent (FA) discovery and to avoid the flooding of the overall ad hoc network, the service announcements are restricted to a limited broadcast zone by using geocast capabilities of VANET routing protocols. For route selection MMIP6 implements a fuzzy-based approach, which considers available information about gateways (i.e., expected disconnection probability, expected number of users for the next IGW, and among others).

3.7 Conclusion

In this chapter we discussed different VANET protocols and we presented the current state of the art for connecting the vehicular networks to the Internet. However, there is still no scalable protocol for connecting vehicular networks to the Internet, which addresses the fast topology changes of VANET, be able to hand-over the connections from one gateway to another seamlessly and benefits from predicting the behavior of vehicles by using their movement parameters at the same time. Next chapter presents our approach which is trying to address all these aspects.

Chapter 4

Connecting Vehicular Networks to the Internet : A Life Time-based Routing Protocol

4.1 Introduction

In this chapter we will introduce our designed protocol to connect vehicular networks to the Internet. We use an infrastructure based network using WLAN 802.11 to provide the Internet access. We assume the network is composed of two types of nodes: vehicles that are stationary or mobile, and gateways that are considered stationary. We suppose that each vehicle is equipped with a positioning system, e.g., a GPS, allowing it to obtain its location. The coordinate of a vehicle u is denoted as (x_u, y_u). Each vehicle is also able to calculate its speed, V_u, and direction, θ_u. Links between vehicles are established if the distance between them is less than their transmission range R. Gateways communicate among each other via the wired network and the Internet. A vehicle can be in the range of a gateway (i.e., it is a direct neighbor) or it can be reached through a multi-hop path as in ad hoc networks.

By a *route* we mean a multi-hop path from a vehicle to a gateway, and a *link* is a direct link between two nodes. Vehicles search for gateways in a proactive way, and use the *link stability* metric to connect to a gateway. They will have the connection over the link with the longest life-time, and always have a list of alternative routes to do seamless hand-over before a link goes down. If a vehicle does not receive any advertisement from the gateways, it should find a new one, and starts to broadcast solicitation messages.

4.1.1 Outline

The rest of this chapter is structured as follows. In Section 4.2 we describe our approach for proactive gateway discovery, and explain how the advertisement messages spread in the network. We also present the algorithm to estimate the life-time of the links and routes based on the movement parameters of vehicles. In section 4.3 we discuss the way vehicles will find a route to a gateway if they have not received any advertisement messages yet. After finding a route to different gateways, vehicles should establish a connection to one of them, section 4.4 presents the idea of connection establishment from a vehicle to a gateway. Section 4.5 explains the way our protocol handle the seamless hand-over when a vehicle is moving outside the range of one gateway and wants to hand-over the connection to the next one. Communicating back from the selected gateway to the vehicle is discussed in 4.6. Section 4.7 concludes this work.

4.2 Proactive Gateway Discovery

The Internet access is provided by gateways implemented in roadside infrastructure units, and vehicles initially need to find these gateways in order to be able to communicate with them. Gateway discovery is hence the process through which vehicles

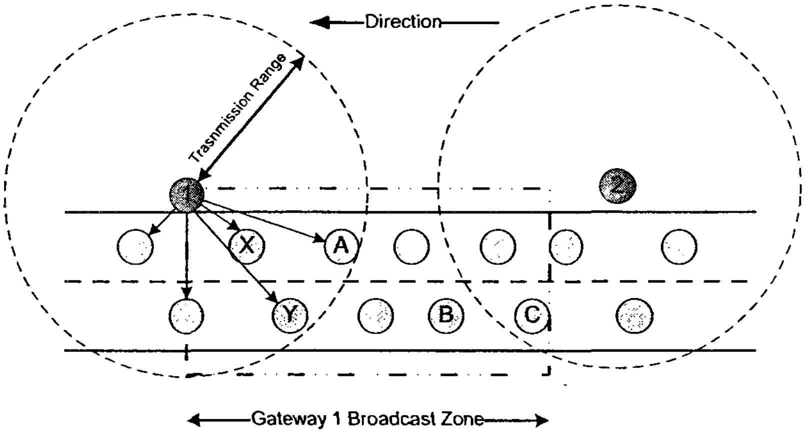


Figure 4.1: A gateway broadcasting an advertisement message, gateway transmission and broadcast zone is shown.

get updated about the neighboring gateways. Gateways periodically broadcast Agent Advertisement messages in a geographically restricted area using geocast capabilities. Gateway Discovery aims at propagating the advertisement messages in the VANET at multiple hops in this area. We call this area the broadcast zone (figure 4.1): a message that originated from a gateway should not be broadcast outside this zone. This area can be a rectangle or a circle[1], and is defined according to the distance between gateways, transmission range of the gateways, and density of the vehicles (whether it is a highway or city, traffic congestion, etc). The specification of the area will be sent along the advertisement messages. For instance, if the broadcast zone is a rectangle with one corners on gateway g_1, and specific length and width, g_1 will send out a message containing following information. First of all, g_1 mentions that the broadcast zone is a rectangle. It will put its own location information in messages as one corner of the rectangle along with the specific length and width of the rectangle. In this way, each vehicle upon receiving the message can compute the broadcast zone and compare it with its own location to make sure that it is inside the computed zone.

[1] It can also be the maximum number of hops to the gateway or even the time to live.

Table 4.1: Agent advertisement message fields

Field	Description
Gateway	Address of the source gateway
Relay	Relay address
Sequence Number	Message Sequence Number
Sender Position	Geographical Position of the sender
Sender Speed	Speed of the sender
Sender Direction	Direction of the sender
RET	Expiration time of the route
Z_m	Message Broadcast Zone

To accomplish the task of proactive gateway discovery, we consider Optimized Dissemination of Alarm Messages (ODAM) [51], which is based on geographical multicast, and consists of determining the multicast group according to the driving direction and the positioning of the vehicles in a geographically restricted area using geocasting capabilities. These messages are then re-broadcast in the network by some particular nodes called *relays.* Figure 4.1 shows a simple scenario, in which gateway 1 starts to broadcast advertisement messages to the vehicles that are in its transmission range. The broadcast zone is considered as a rectangle here, and has an intersection with the transmission range zone of gateway 2. In this case, messages from gateway 1 will be broadcast through multiple hops to some of the nodes which are connected to gateway 2.

Each advertised message contains the gateway address, relay address, message sequence number, broadcast zone, and the stability parameters. Stability parameters will be used by each vehicle receiving the message to predict the link life-time, which will be explained later. These parameters are the sender position, sender speed, sender direction and the estimated route expiration time (RET). When gateways are creating a message, they set the relay address to their own address and set the RET to a large value. The message structure is shown in table 4.1.

4.2.1 Stability metric

In vehicular networks, vehicles are connected either directly to a gateway or using multiple hops. If they have a direct connection to the gateway using a single link, as long as that link is up and working the connection is alive. If they have a connection over multiple hops, the connection is alive as long as each single link is up and working. When a link goes down, the route to the gateway will fail and the vehicle will be disconnected from the network. We can therefore say that a route life-time is the minimum life-time of the links along that route.

We will use the mobility prediction mechanisms suggested in [78] to predict the *Link Expiration Time (LET)* of the adjacent vehicles, and will apply it to predict the *Route Expiration Time (RET)* sequentially. We assume that all nodes in the network have their clock synchronized; therefore, if the motion parameters of two neighbors are known, we can determine the duration of the time that these two nodes will remain connected. Let (x_i, y_i) and (x_j, y_j) be the coordinates of vehicles i and j which are moving in directions θ_i, θ_j $(0 \leq \theta_i, \theta_j < 2\pi)$ with the speed of v_i and v_j respectively, and let r be the transmission range. We can estimate the amount of time they will stay connected as:

$$LET_{ij} = \frac{-(ab + cd) + \sqrt{(a^2 + c^2)r^2 - (ad - bc)^2}}{a^2 + c^2} \tag{4.1}$$

where,

$$\begin{aligned} a &= v_i \cos\theta_i - v_j cos\theta_j, \\ b &= x_i - x_j, \\ c &= v_i \sin\theta_i - v_j \sin\theta_j, \\ d &= y_i - y_j \end{aligned}$$

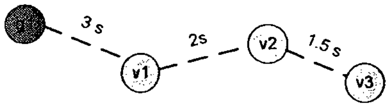


Figure 4.2: An example of how we compute the route life-time.

Note that when $v_i = v_j$ and $\theta_i = \theta_j$, then $LET_{ij} = \infty$. For example, vehicles can use the north axis as a reference for the direction angle and a predefined two-dimensional coordinate system for positions. LET_{ij} is hence the *Link Expiration Time* of the link between vehicles i and j.

Since gateways are stationary, they do not move towards a specific direction and their speed is 0; we always assume that the direction of a gateway is the same as the road direction beside which it is deployed. For example, on a two-way highway that lies in the North-South direction, base stations along the North direction will broadcast "North" as their direction and the others will broadcast "South".

The gateway direction can be used to prevent vehicles from connecting to the gateways on the other side of the road, or gateways along the other roads at the intersections. While receiving the broadcast messages, vehicles check the direction broadcast along with the advertisement messages to see if they come from a gateway along the same road in the same direction as they are.

Let R_{n-1} be a route, which consists of $n-1$ links l_{01}, l_{12}, ..., $l_{(n-2)(n-1)}$ between n vehicles $0, 1, ..., n-1$. To compute the *Route Expiration Time (RET)* we should find the link which expires first, hence:

$$RET_{n-1} = \min\{LET_{ij}\}, i = 0, \ldots, n-2, j = i+1 \tag{4.2}$$

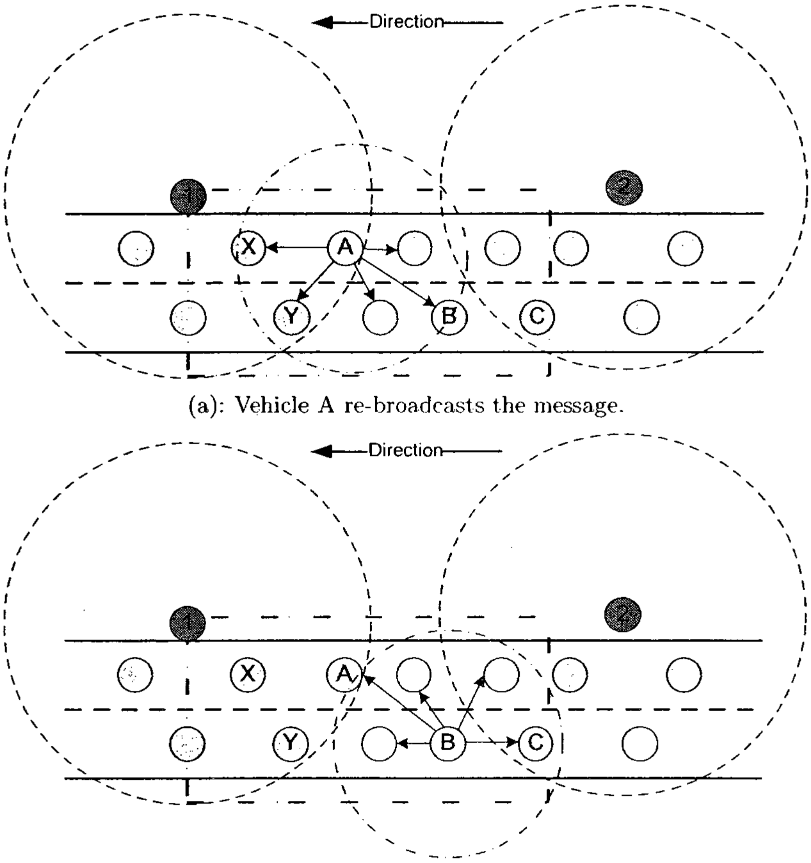
To find the minimum link life-time along a route, we are taking a sequential approach. This means that each vehicle finds the expiration time of the link between itself and the sender, and compares it to the RET integrated into the message. If the link expiration time is less than the route expiration time, so the new RET will be set to the computed *LET*. In this way, as the message is getting forwarded through multiple hops, the route expiration time is getting updated. Figure 4.2 illustrates a scenario where vehicle v_3 is connected to gateway g_1 through vehicles v_2 and v_3. The life-time of each link is written over the link. The route life-time will be the minimum link life-time of the links that construct the route, which is 1.5 in this case.

4.2.2 Relays and Re-broadcasting

As mentioned earlier, not all the vehicles in our protocol re-broadcast the advertisement messages sent by the gateways; instead only some particular vehicles called *Relays* forward such messages to other vehicles. For example, each vehicle may schedule transmissions as in ODAM [51], and while one node re-broadcasts the message, it suppresses other nodes from re-broadcasting the same message. It has been shown in [51] that this helps in reducing the overhead and collisions in the network; future broadcast messages will not flood the network and this prevents broadcast storms from happening.

Figures 4.3(a) and 4.3(b) show how the advertisement messages spread through the network. Vehicles A and B are the relays in this case, and re-broadcast the message. The message gets re-broadcast until it reaches the end of the broadcast zone. In figure 4.3(a), vehicle A is the first one that broadcasts the message to its neighbors and as a result it becomes the relay of its own zone. Vehicles X and Y also receive the advertisement message from gateway 1, but when they receive the re-broadcast message from A, they will not broadcast it any further and the message gets discarded. Hence, the relay will always suppress other vehicles from broadcasting the same message multiple times.

In our work, each vehicle upon receiving the agent advertisement messages, retrieves the broadcast zone (Z_m) and the sender direction from the received message. If it is not in the broadcast zone and the sender direction is different by more than



(a): Vehicle A re-broadcasts the message.

(b): Vehicle B re-broadcasts the message.

Figure 4.3: An example that shows how the advertisement messages spread in the network.

$\pi/4$, it will discard the message. A vehicle estimates the expiration time of the link over which it received the message, by applying the stability parameters integrated into the message.

Here, as explained in the sequel, the selection of the next hop is performed by means of contention, in a similar manner to the Contention Based Forwarding (CBF) approach [13]. Initially we describe the Contention Based Forwarding in detail, next since our approach is very similar to CBF, then our approach will be explained.

Contention Based Forwarding

Contention Based Forwarding (CBF) [13] is a greedy forwarding approach without the help of beacons to update the nodes about the position of the neighbors, and does not require the maintenance of information about the direct neighbors of a node. The authors of [13] discussed the fundamental problem of inaccurate position information which is always present in a position-based routing approach. A neighbor selected as a next hop may have moved and may not be in transmission range of the sender any more. The authors showed that this leads to a significant decrease in the packet delivery rate with increasing node mobility and to a high load on the wireless channel due to several MAC layer retransmissions. One way to avoid such problem is to increase the beaconing frequency as the mobility increases. However, this will put higher load on the network.

CBF suggests that, instead of receiving the position information from all neighbors of a node, all the direct neighbors of a forwarding node will participate in the next hop selection based on their location at the time of forwarding. CBF performs better than normal greedy approaches in case of using accurate position information and eliminating the beacon overhead. CBF consists of two parts: the *selection* of the next hop which is done by using contending, and *suppression* that is used to reduce the chance of selecting more than one node as the next hop by accident.

In CBF, first the forwarding node broadcasts the data packet to all the neighbors, instead of using recorded information and uni-casting it to the corresponding MAC address. Then, the neighbor competes with each other in order to acquire the "right" to forward the packet (*contention period*). Finally, the node that wins the contention *suppresses* the other nodes and thus establishes itself as the next forwarding node.

A standard approach for decentralized selection of one node out of a set of nodes is by means of timers. Timer-based contention requires that each node sets a timer with a random value. Once the first timer expires, the corresponding node sends a response and the timer of all other nodes will be canceled and their responses will be suppressed. However, using this contention based approach, more than one node may respond at the same time, even with the presence of a 'good' suppression mechanism. It happens when the difference between the timeout values of two nodes become smaller than the time required for suppression.

For implementing such a timer-based mechanism for contention, all nodes receiving a forwarded packet check if they are closer to the destination than the forwarding node. In that case, a random (exponentially distributed) timer is set to start the contention and the first node that responds is selected as the next hop. The authors proposed the value for the timers based on how much progress a node provides toward the destination instead of setting them randomly. In this way, nodes that make more progress towards the destination than other nodes will have higher chance to forward the packet.

To greedily minimize the remaining distance to the destination, the progress P is defined as:

$$P(f, z, n) = max\left\{0, \frac{dist(f, z) - dist(n, z)}{r_{radio}}\right\} \tag{4.3}$$

where f is the position of the forwarder, z the position of the destination and n the position of the considered neighbor. *dist* is defined as the Euclidean distance

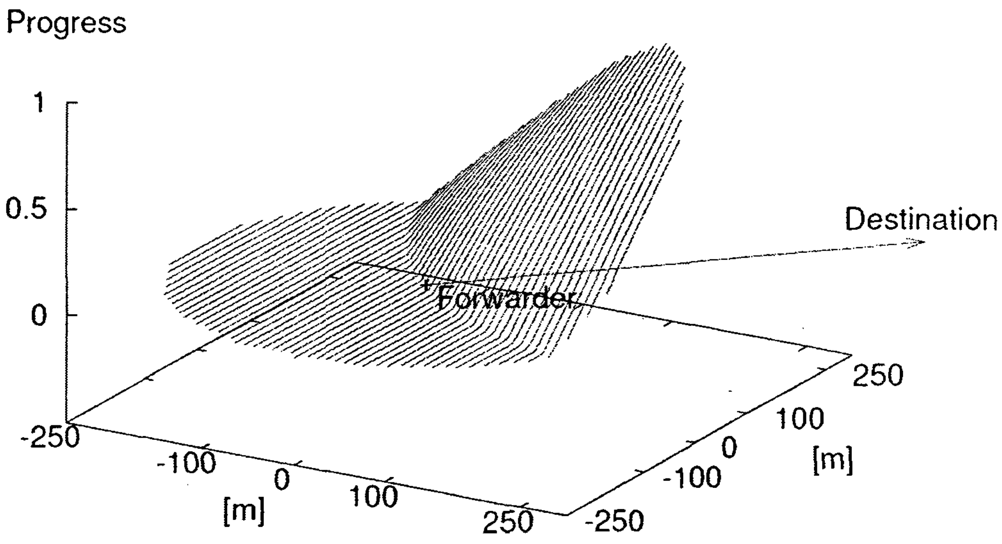


Figure 4.4: Packet Progress (transmission range 250m)

between two positions and r_{radio} is the nominal radio range.

Figure 4.4 illustrates how well suited a node is for being the next hop, depending on its location[2]. A progress value (P) of 0 indicates that a node is unsuitable while a value of 1 is optimal and is reached if the node is located at the perimeter of the transmission range circle of the forwarding node, on the line that connects the forwarding node to the destination. Thus P increases linearly from 0 to 1 with the progress that a node at this position would provide for the packet.

For the contention in CBF, the authors used the following timer runtime:

$$t(P) = T(1 - P) \tag{4.4}$$

where T is the maximum forwarding delay. This makes sure that the node with the largest progress is selected as next hop. Since the runtime of the timer only depends on the remaining distance to the destination it is identical for all nodes that are located on the same circle around the destination. A packet duplication may occur in the following situation: if the best suited node has a progress of P_1 and there exists

[2] This figure was taken from [13]

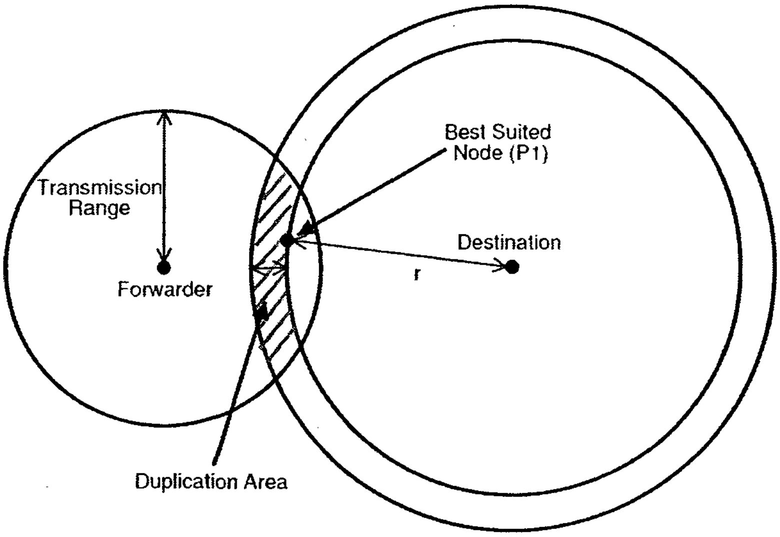


Figure 4.5: Duplication area

at least one node with a progress of P such that $t(P) - t(P_1) < \delta$, where δ is the minimum time interval needed for suppression, then at least one packet duplication occurs. All nodes with progress P and

$$P_1 \geq P \geq 1 - \frac{\delta + T(1 - P_1)}{T} = P_1 - \frac{\delta}{T} \tag{4.5}$$

are within this so-called *duplication area* and cannot be suppressed, as shown in figure 4.5.

Three suppression schemes are suggested:

- **Basic suppression scheme.** When the timer at a node expires, by default the node assumes that it is the next hop and immediately broadcasts the packet. When another node receives this broadcast and still has a timer running for the packet, the timer is canceled and the packet will be dropped. Depending on where the initial next hop is located, other nodes may be out of transmission range and will thus not be suppressed. In the worst case, up to three copies of the packets may be forwarded.

- **Area-based suppression.** In order to avoid the extra packet duplications from the basic suppression scheme this scheme was proposed to artificially reduce the area from which the next hop is selected. This reduced area is called the *suppression area* and the algorithm *area-based suppression.* The key idea is to choose the suppression area such that all nodes within that area are in transmission range of each other, avoiding extra packet duplications as they may appear in the basic suppression scheme.

- **Active selection.** While area-based suppression eliminates the packet duplications caused by nodes not being in transmission range of each other it does not prevent packet duplications caused by the time required to perform the suppression. Active selection of the next hop prevents all forms of packet duplication at the cost of additional control messages.

Contention Based Forwarding Vs. Our Protocol

In CBF, the next hop is selected through a distributed contention process based on the actual positions of all current neighbors. For the contention process, CBF makes use of biased timers. To avoid packet duplication, the first node that is selected suppresses the selection of further nodes. CBF uses the amount of progress that each packet makes towards a certain destination to set a runtime timer. The authors used a progress function that measures the progress amount and they set the timer based on the result. However, in our work we want to spread the beacons (of the gateways) in the broadcast zone and there is no specific destination. We are also interested in the stability of the links between the sender and the receivers rather than only how much progress they have made towards a final destination. Therefore, we need to design a new function which fulfills our requirements, instead of the progress function suggested in [13].

4.2.3 Relay Selection

The relay should be the node that has the most stable link with the sender (the vehicle from which the message has arrived); furthermore, we are also interested in the amount of progress that the message has made in the opposite direction of the movement (the message here is an advertisement message broadcast by the gateway, as explained in 3.1). However, the latter has to be less effective than the former due to the nature of our protocol which tends more to build a stable path instead of reducing the number of hops. By combining these two features, we would be certain that the chosen path is the most stable one with fewer hops. The amount of progress in our protocol is useful if we have two or more vehicles with the same LET, in such case the amount of progress will decide which node should rebroadcast the message. To define the replacement function for the CBF progress function, first we consider the stability metric and we study this scenario, then we add the second part to come up with the final function.

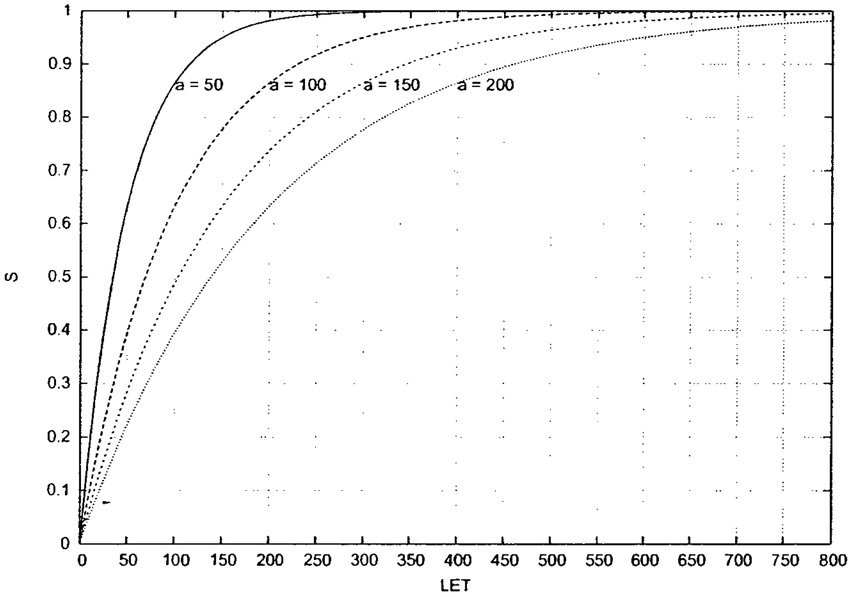


Figure 4.6: Effect of selecting different values of a on function S

The replacement function, which for now we call it the "stability function", must be dependent on LET, which lies in $(0, \infty]$, and should be mapped to $(0, 1]$. Note that the longer is the link life-time, the closer should be the result of this function to 1, and conversely the smaller is the link life-time, the closer to 0 this function should be. For this purpose, we decided to take advantage of an exponential function that satisfies the given criteria. Denote the stability function:

$$S = 1 - e^{\frac{-LET}{a}} \tag{4.6}$$

where a is a constant that defines the rate at which the function is rising; the lower is a, the faster the function rises as shown in figure 4.6. For the contention over link life-time we select the timer as follows:

$$t(S) = T(1 - S)$$

where T is the maximum forwarding delay. When receiving a message, a vehicle will wait for the amount of time that is computed by the timer, before re-broadcasting the message. If during this time it receives a message originated from the same gateway with the same sequence number (that is another vehicle has re-transmitted the message), it will cancel the timer and discard both messages. Otherwise, it re-broadcasts the message after the timer has expired, becomes a relay and the message sent from this node will suppress other nodes. This makes sure that the node with the longest life-time is always selected as the next relay.

Note that a packet duplication may still occur if the LET of two vehicles is very close to each other, that the difference between the timers become less than the time needed for suppression. This means that if the node with largest LET has a stability of S_1, then there exists at least one node with a stability of S such that $t(S) - t(S_1) < \delta$, where δ is the minimum time interval needed for suppression. All nodes with stability S and

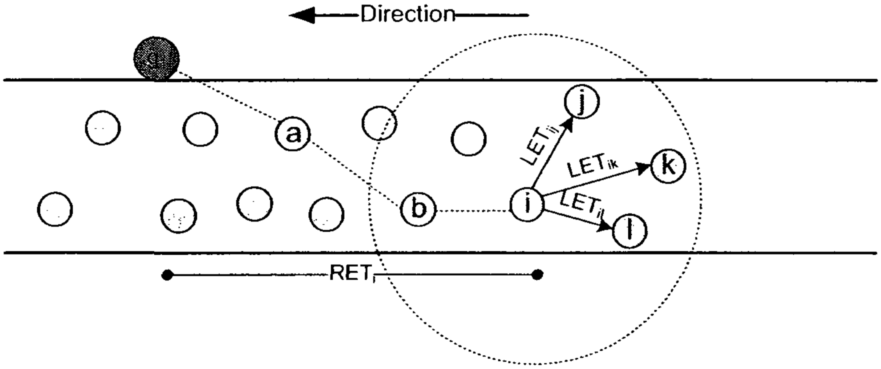


Figure 4.7: How to select a

$$S_1 \geq S \geq 1 - \frac{\delta + T(1 - S_1)}{T} = S_1 - \frac{\delta}{T}$$

are within a *duplication area* and cannot be suppressed. For example. if two vehicles in the transmission range of the sender move in the same direction and with the same speed, their *LET* will be close to each other, and then the result of S and $t(S)$ will be close as well, and more than one instance of the packet will be retransmitted. Hence, we need another function to differentiate between the vehicles with *LET*s close to each other. Before we explain the second function, we elaborate on how to select a.

Observe that for values of *LET* much larger than *RET*, it does not matter which vehicle will rebroadcast the message, since they cannot improve the route life-time, which is defined as the minimum value of *LET*s along the path. For example, in figure 4.7, we assume that LET_{ij} and LET_{ik} are much larger than RET_i which is the route life-time from gateway g_1 to vehicle i. Either vehicle j or vehicle i are eligible to rebroadcast the message. For such large values of *LET*, our stability function should act in a way that the result of S_{ij} and S_{ik} is close to each other, to eliminate the chance of rebroadcasting by one of these vehicles before the other one.

Accordingly, we decided that our stability function (defined in (4.6)) should yield results close to each other for any two links with LETs larger than twice the RET. In other words, if $LET_{ij}, LET_{ik} \geq 2 \times RET_i$ then the function should yield $S_{ij} \simeq S_{ik}$ (and hence $t(S_{ij}) \simeq t(S_{ik})$). In such case, both vehicles j and k will broadcast the received message at the same time, which results in duplication. Therefore, one needs to introduce another function to decide which vehicle (among j and k) must rebroadcast the message, as explained shortly.

Recall now from (4.6) that the stability function depends on a parameter a whose value is not determined. a should be selected such that S satisfies the aforementioned properties; observe from figure 4.6 that for $LET \geq 4 \times a$, (4.6) yields $S \simeq 0.98$ and for $LET_{ij}, LET_{ik} \geq 4 \times a$ we obtain $|S_{ij} - S_{ik}| < 0.02$. This shows that $4a$ can be selected as a cutoff after which the values of stability are very close to each other. Based on our discussion, we obtain two necessary conditions that S should satisfy:

$$LET \geq 2 \times RET$$
$$LET \geq 4a$$

The first one shows us what are the large values of LET, for which we want to make the results of the functions to be close to each other. The second one is the point after which we are certain that the difference between the results of the stability function will be very small. From these inequalities we can find the proper value for a:

$$2 \times RET = 4 \times a$$
$$a = \frac{RET}{2}$$

Now we rewrite (4.6) as:

$$S = 1 - e^{\frac{-2LET}{RET}} \tag{4.7}$$

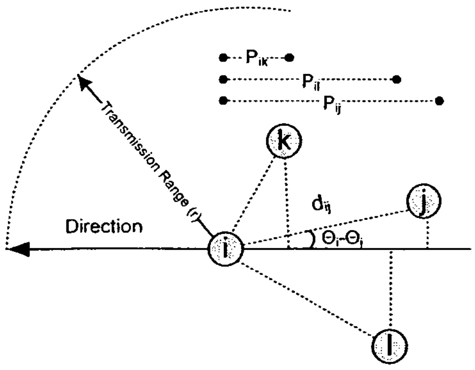


Figure 4.8: Progress in the opposite direction of the movement

After selecting a proper value for a, we need to introduce the second function to eliminate the duplications as discussed earlier. The progress that the packet makes in the opposite direction of the movement seems to be proper for this purpose. As it can be seen in figure 4.8, we define the second function as follows:

$$P = \frac{cos(\theta_i - \theta_j) \times d_{ij}}{r} \tag{4.8}$$

where d_{ij} is the distance between vehicle i (sender), and vehicle j (current receiver), and r is the transmission range of vehicles. θ_i and θ_j are respectively the angles between the direction of the sender and the receiver with the north axis. P will yield a value between 0 and 1; the further is the receiver from the sender, the closer is the result to 1. In this case, whenever two vehicles have the same link life-time with the sender, the contention will change from selecting the longest link life-time to the largest progress that has been made in the opposite direction of the movement. In Figure 5, P_{ij}, P_{ik} and P_{il} show the progress for vehicles i, j, l respectively. Vehicle j has the largest progress, and P_{ij} will be larger than others. In order to get the final progress function, we should combine S and P together. However, P should not be as effective as S for next hop selection. We take advantage of a weighted mean to reduce the effect of P in the final function. Denote the final function:

$$F = \alpha \times S + (1 - \alpha) \times P \tag{4.9}$$

In order to give more weight for link stability, α may be selected in $(1/2, 1]$. In a subsequent chapter we perform some simulations to find the proper value of α. Finally, for the contention in our protocol we select the timer runtime as:

$$t(F) = T(1 - F)$$

where T is the maximum forwarding delay. We will be sure that the next hop will be the one with the longest life-time and the largest progress in the opposite direction of the road.

We will try to predict the LET along each hop of the route to predict the route expiration time. As a vehicle receives a message, it predicts the life-time of the link over which it received the message, and compares it to the RET extracted from the message. The minimum value will be the new RET for the current route. For two successive relays j and $j+1$, RET_{j+1} can be obtained as follows:

$$RET_{j+1} = min(RET_j, LET_{j+1})$$

where RET_j is the route life-time computed by vehicle j. Initially, the relay field in the message is set to the address of the gateway and RET is equal to ∞. When the vehicle wants to re-broadcast the message, the new RET is included in the message before it is sent out.

Note that, since most of the roads (highways or city streets) have two directions, one possibility for the gateway discovery will be to take advantage of the vehicles that move in the opposite direction of the current vehicle to broadcast the advertisement messages. In *ODAM*, which is a protocol for dissemination of alarm messages, it has been mentioned that using the vehicles in both directions will yield a great help in sparse scenarios, where the number of vehicles on the road is very small. Indeed, for the sake of spreading messages in the network, it makes great sense to use all the vehicles on the road. However, in the scenario of establishing a connection to gateways (as in our case), it is not efficient to count on such vehicles as relays. The reason is very simple, since the relative speed between the vehicles that move in the opposite direction is very high in comparison to the vehicles that move in the same direction, and the life-time of the links will be as a result very small. In essence, these unstable links are not good for a protocol that seeks robustness in the connections and requires long life-time links.

4.3 Reactive Gateway Discovery

In addition to the proactive gateway discovery, a reactive gateway discovery can be executed if a vehicle does not hear any agent advertisement messages from its neighbors. In this case, an agent solicitation message is broadcast by exactly the same mechanism as the agent advertisement messages, with stability metrics as explained above. The only difference is that the broadcast can be stopped when the solicitation messages reach a vehicle that is already aware of a route to a gateway or reaches a gateway. In such case, the reply is sent directly to the vehicle which is willing to connect to the Internet. If there were more than one reply, the vehicle will select the most stable route. If the routes have equal life-times, the route with minimum number of hops to the gateway will be selected.

Table 4.2: Routing table

RET (sec)	Next hop	Seq_num	Gateway
R	N	s	g

4.4 Route Establishment to the Gateway

As explained, vehicles receive advertisement messages either directly from gateways or by means of other vehicles. In this way, each vehicle will have access to one or more gateways and should decide to which gateway it should send its data. Each vehicle keeps a routing table to manage the different routes to different gateways. The routing table contains the route expiration time, next hop, message sequence number and the gateway address as shown in table 4.2. Vehicles compute the new RET, and get values of other parameters directly from the received message.

When receiving a message, each vehicle acts as a router and attempts to update its routing table. If it does not have any entry with the address of the gateway from which the message was sent, it simply adds an entry to the routing table. If it already has an entry corresponding to the gateway address, it checks the message sequence number. Messages with higher sequence numbers have newer information and should be inserted into the table replacing the old information. However, if a message has the same sequence number as the entry in the routing table, we check to see if it arrived from a better route with greater route life-time. In this case, the vehicle will update the routing table with the information extracted from the message. Routes are removed from the routing table when their life-time expires.

4.5 Seamless Hand-over

Vehicles movements in VANET are predictable, since they are moving on a road and the direction of the road is known. Gateways are broadcasting their messages to the opposite direction of the route, and the vehicles which are moving towards them will be aware of their existence. In our protocol, thanks to the relays, messages can be broadcast at multiple hops, and each vehicle knows a route to a gateway prior to reaching the transmission range of that gateway. By managing a routing table which contains the information of the gateways and the approximate life-time of the routes, vehicles can predict the time when their connection with the gateway ends. They can establish a connection to another gateway before they lose their current connection, and can seamlessly hand over the connection to the next gateway.

Vehicles always select the route with the largest life-time and establish a connection over it. When they determine that the route is about to expire, or the "critical time" is reached, they look up the gateway table (table 4.2), to find the most stable route available to the next gateway, and start establishing a connection over that. After the connection has been established, it will hand-over the current connection to the new gateway. The "critical time" is defined as follows:

$$T_c = RET - T_d \tag{4.10}$$

Where T_d is the delay experienced by the last packet which has arrived along the route. Since the network load conditions will change from time to time during the connection, the delay will also change accordingly. By using the latest arrived packet to calculate T_c, the scheme is adaptive to changing network conditions and the vehicle will correctly take action in a timely manner.

4.6 Gateway Communication with Vehicles

Earlier, we explained how to establish routes between vehicles and gateways and select the most reliable path to the gateway. Next, we have to specify a procedure which enables gateways to send data downstream to the source node. For this purpose, we assume that each intermediate vehicle is managing a routing table in which it caches the information pertaining to the route used by the source node to reach this intermediate vehicle. Besides, each vehicle sends the route life-time information along with the transmitted message. While vehicle A (or gateway A) receives a data packet from vehicle B, it stores the information of vehicle B and the source node, inside the routing table and add the route life-time information to this table as well. If there is already an entry related to vehicle B in the routing table of A, A checks the new route life-time; if they match, it will do nothing, but if the new life-time is longer, then A replaces the old information with the newly received information in the table. After this route life-time expires, vehicle A will remove the entry related to vehicle B from its routing table.

Hence, as the data packet is forwarded towards the specific gateway, each vehicle along the route will have the information related to the previous hop. When the gateway receives the data packet (assume this packet is a request to download some information from the Internet, e.g., a web page access), it retrieves the requested information from the Internet and will try to send this information back to the source node (requester). For this purpose, it looks up the source IP address in the routing table and find the node from which it received the data packet. Each intermediate vehicle by receiving the response, looks up the source IP address in the routing table, and find the next downstream hop towards the source node.

One challenge which might arise is what will happen if the route life-time has expired, or the vehicle gets out of the gateway range before the gateway retrieves the information from the Internet. Here, the gateway prior to sending back the response, it first checks the life-time of the route from which it received the data packet. If the route is still valid, the gateway sends back the response as explained, otherwise, it has to take an alternative approach, which will be explained below.

When the route life-time expires, immediately vehicles check their gateway table and switch to the next available route towards the gateway. After this, they send an *update* message that contains no information back to the gateway, which will cause all the intermediate vehicles to update their routing tables with the new information. Also, the update message will update the gateway with the latest information about the new route available toward this particular node. Accordingly, each gateway has the latest information about all the nodes in the network and if one route fails, they know which routes should be used to reach the source node. However, one exception is when the source node hands over the connection to a route which relates to the next gateway on the road. In this case, the current gateway will not be updated with the new information, after waiting for a while it will forward the response to the next gateway, and the second gateway will forward the packet to the source node as explained earlier.

4.7 Conclusion

VANETs will play an important role in the future, and communicating with road infrastructure units is one aspect that should be covered in order to provide specific services such as Internet access. We proposed a predictive gateway selection scheme, which uses vehicles movement parameters to select the path with longest life-time by predicting the future location of neighbors of a vehicle. This helps to have more stable routes to the gateways, and it helps to maintain better quality of the network. In the following chapter, we evaluate the performance of our protocol in highway scenarios.

Chapter 5

Performance Evaluation

In this chapter, we evaluate the performance and effectiveness of our protocol using NS-2 [79]. We have compared our work with AODV+ [80] and Greedy Perimeter Stateless Routing (GPSR) [15]. AODV+ is a modified version of AODV [14] for connecting mobile ad hoc networks to wired networks. GPSR is a geographic routing protocol which uses positions of nodes to forward the packets in a greedy manner. First, we perform some simulations in order to find the proper value for α, as stated in (4.9). Then, we analyze and evaluate our proposed protocol by investigating the effects of changing the mobility of nodes and density of nodes on the road. We also study the effect of changing the transmission range of wireless devices on the performance of our protocol.

5.1 Simulation Environment

5.1.1 Mobility Model

Depend on the type of the road that the vehicles are moving in, city or highway, two different scenarios can be studied: city scenarios and highway scenarios. In a city scenario, vehicles move in a network of roads including traffic lights, intersections, stop signs and other possible obstacles that might appear in a city area. Buildings and other obstacles can block the transmission in an urban area. On the other hand, in a highway scenario there is not as many obstacles as there is in city scenarios and the traffic is flowing smoothly.

There are two types of mobility models for VANET: micro-mobility and macro mobility models. Macro-mobility models take into account the road structure (unidirectional, bidirectional, and number of lanes), road characteristics (speed limits and vehicle classes limitation) and the presence of traffic signs. Micro-mobility models take care of the vehicle speed, acceleration and various vehicle behaviors in different situations.

Our protocol is designed specifically for highway scenarios, and we evaluate our protocol using a highway scenario. To simulate a VANET scenario rather than implementation and simulation of the designed protocol using a network simulator, the mobility model should be simulated as well. Generating the mobility model is independent of the network simulator program and should be done using an application which is designed for such purpose. For the mobility scenario we used MOVE [81] a mobility model generator for vehicular networks, which facilitate users to rapidly generate realistic mobility models for VANET simulations.

MOVE is developed on top of the open source micro-traffic simulator SUMO (Simulation of Urban MObility) [82]. SUMO is a micro-mobility traffic generator which is designed to handle large road networks. MOVE is a JAVA based application which receives some basic information about the road structure, speed limits and number of the vehicles on the road. MOVE passes this information to SUMO, in order to generate realistic traffic simulation scenarios. Then MOVE converts these movement information to NS2 trace file format, and NS2 can immediately use this trace file for the final simulation.

Our generated highway scenario is a 8km highway with two lanes, both in the

Table 5.1: Mobility features

Type of road	Highway
Length of road	8 Km
Number of lanes	2 lanes in the same direction
Maximum speed	Varies between 15, 20, 30 and 40 m/s
Number of vehicles	Varies between 100, 200, 300 and 400 vehicles
Number of RSUs	8
Distance between the RSUs	1 km
Simulation period	500 s
Warm up period	150 s

same direction (as explained earlier vehicles moving in the opposite direction can not improve our life-time based protocol). It is possible to set the maximum speed of the vehicles on the road in MOVE, using this feature we provided different speeds for different simulation scenarios, which will be presented in the following section. Moreover, it is possible to change the number of the vehicles on the road by using MOVE, and it helped us to vary the number of nodes in different scenarios.

Vehicles are connecting to the roadside infrastructure units beside the roads. There are 8 infrastructure units beside the highway which are located 1km apart from each other (since the transmission range has been set to 250 meters). The transmission range of gateways do not overlap with each other in our simulation. These infrastructure units are fixed network nodes which have been generated using NS2, and are considered to be the base station for the vehicles in their broadcast zone.

The simulation period should be set in both the network simulator and the mobility generator. Using the provided simulation time, the mobility generator determines the location of each vehicle at different points in the time starting from one end of the highway to the other end. The simulation period in our work is 500s. When the simulation begins, the highway is empty and no connection has been established yet among vehicles or between vehicles and infrastructure units. We wait for 150s after the beginning of the simulation as the warm up period, for the traffic to flow

Table 5.2: Network parameters in NS2

Channel type	Channel/WirelessChannel
Radio-propagation model	Propagation/TwoRayGround
Network interface	Phy/WirelessPhy
MAC	Mac/802_11
Interface queue	Queue/DropTail/PriQueue
Antenna model	Antenna/OmniAntenna
Max packet in interface queue	50

smoothly and for the network to become stable. All these features are summarized in table 5.1.

We did not use any location service in the simulation, our work does not require a location service since the location information is broadcast through the network using the broadcast messages. Also for GPSR we assumed that nodes have previous knowledge of the gateways location, since here we are just interested in the routing results of GPSR. Each node gets its location information from NS2.

5.1.2 Network Parameters

As explained earlier DSRC (Dedicated Short Range Communications) [9], is the suggested MAC protocol for vehicular networks, however it has not been standardized yet and is not available for network simulators including NS2. However since DSRC is a family member of IEEE 802.11x protocols, we have implemented all the functionalities based on IEEE 802.11 MAC with two ray ground radio propagation model and 2MBit/s bandwidth. The transmission range of vehicles and base stations has been set to 250m as default. The type of the antenna is omnidirectional as can be found in NS2. A summary of these parameters is provided in table 5.2.

For performance evaluation, 10 vehicles are selected randomly to send data to a node that is part of the wired network and is connected to all the base stations. Each vehicle starts to move from one end of the highway to the other end, and as its speed increases it starts to send packets towards a node located outside the VANET network. Each source sends UDP packets of 512byte size with the interval of 4.0s (i.e., one packet every 4 seconds).

To simulate our protocol, the broadcast interval has been set to 5s and the broadcast zone has been considered to be a circle with a radius of 1000m. We choose T to be 3.75ms, which proved to be a useful setting in [13].

AODV+ is used in hybrid gateway discovery mode with 5s interval, which means that it uses both proactive and reactive gateway discovery methods to find the proper gateway. Also advertisement zone for AODV+ has been set to 3 nodes. This means that an advertisement message will be only broadcast 3 times in the network, and nodes located further than 3 hops from a specific node have to send a route request message in order to find a route to that specific node.

The beaconing interval of GPSR is set to the default value which is 3s. We do not use any location service, and the destination coordinates are provided by the simulator's global knowledge.

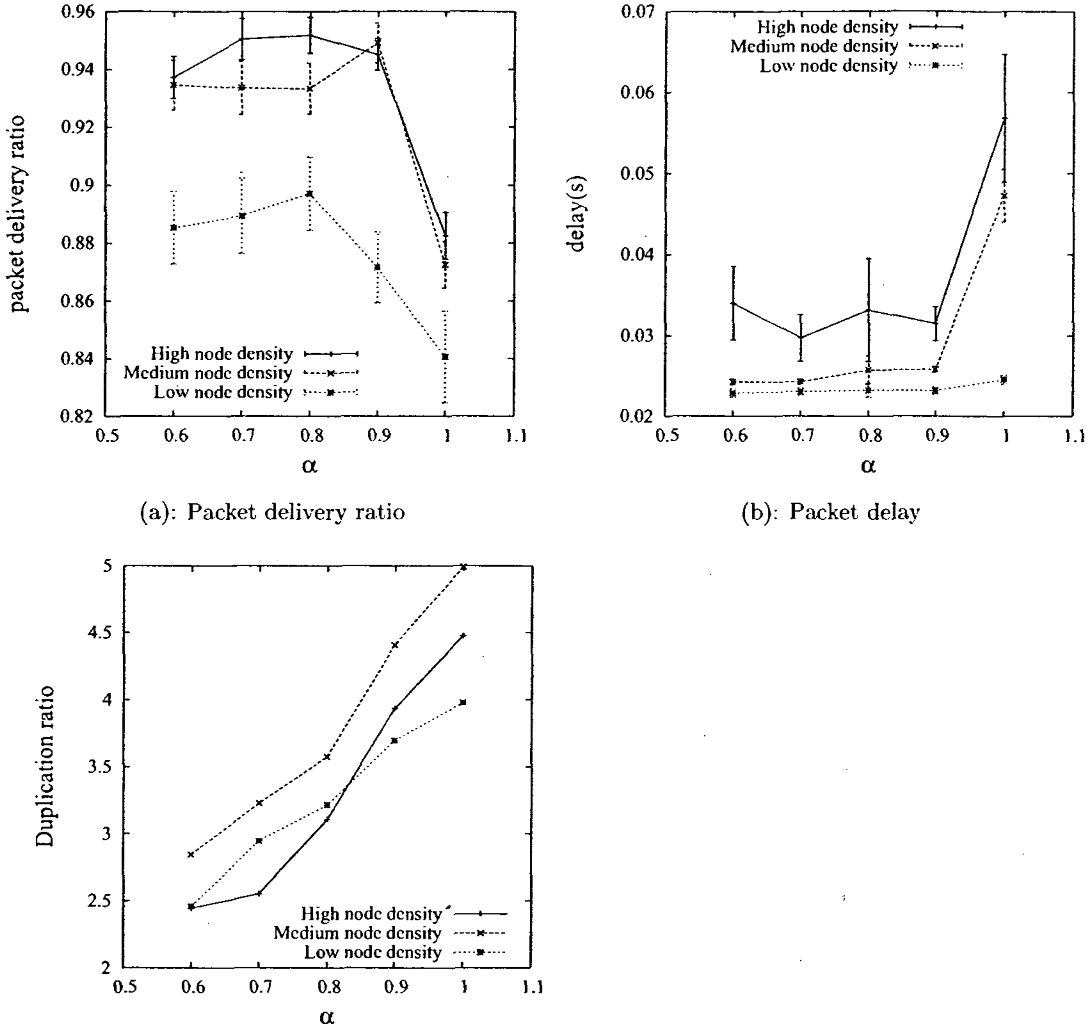
The metrics that we used for evaluation are:

- **Packet delivery ratio (PDR).** The number of data packets received by the destination node, divided by the number of data packets sent by the source nodes.

- **Packet delivery delay.** Which is the average latency between originating a data packet till the packet is received by the destination.

- **Normalized packet duplication metric.** We used the normalized packet duplication metric to choose the best value for α. The normalized duplication ratio is the number of the control messages that has been re-broadcast by more than one node over the whole number of control messages.

- **Overhead.** By overhead here, we mean the total size of the transmitted control messages by a routing protocol in the network.



(a): Packet delivery ratio

(b): Packet delay

(c): Duplication ratio

Figure 5.1: Simulation results under different network settings in order to find α

5.2 Simulation Results

In this section, first we are going to find a proper value for α as explained earlier in previous chapter. Then we will provide some evaluations for the value of a that we suggested in chapter 4. At the end we evaluate our suggested protocol using the value of α that we found in the first part.

5.2.1 Finding α

To find a proper value for α we simulated different scenarios and we changed the value of α and set it to $0.6, 0.7, 0.8, 0.9$ and 1. Since we are trying to improve the life-time of the connection, we avoid using values for α that are less than 0.5. We try to find a proper value for α by changing the node density in the highway scenario.

In all these scenarios the speed of the vehicles has been set to 30m/s, and we varied the node density. Figures 5.1(a), 5.1(b) and 5.1(c) respectively show the packet delivery ratio, delay and the ratio of the duplicated messages for different values of α with different node densities.

As it can be seen from the simulation results, the number of control message duplications goes up, as we increase α. The reason is that by increasing α, P will be less effective as stated in (4.9), so the difference between the waiting time for the nodes with a large value of LET will be very small. This results in multiple rebroadcasting of the same message and increases the number of duplications in the network.

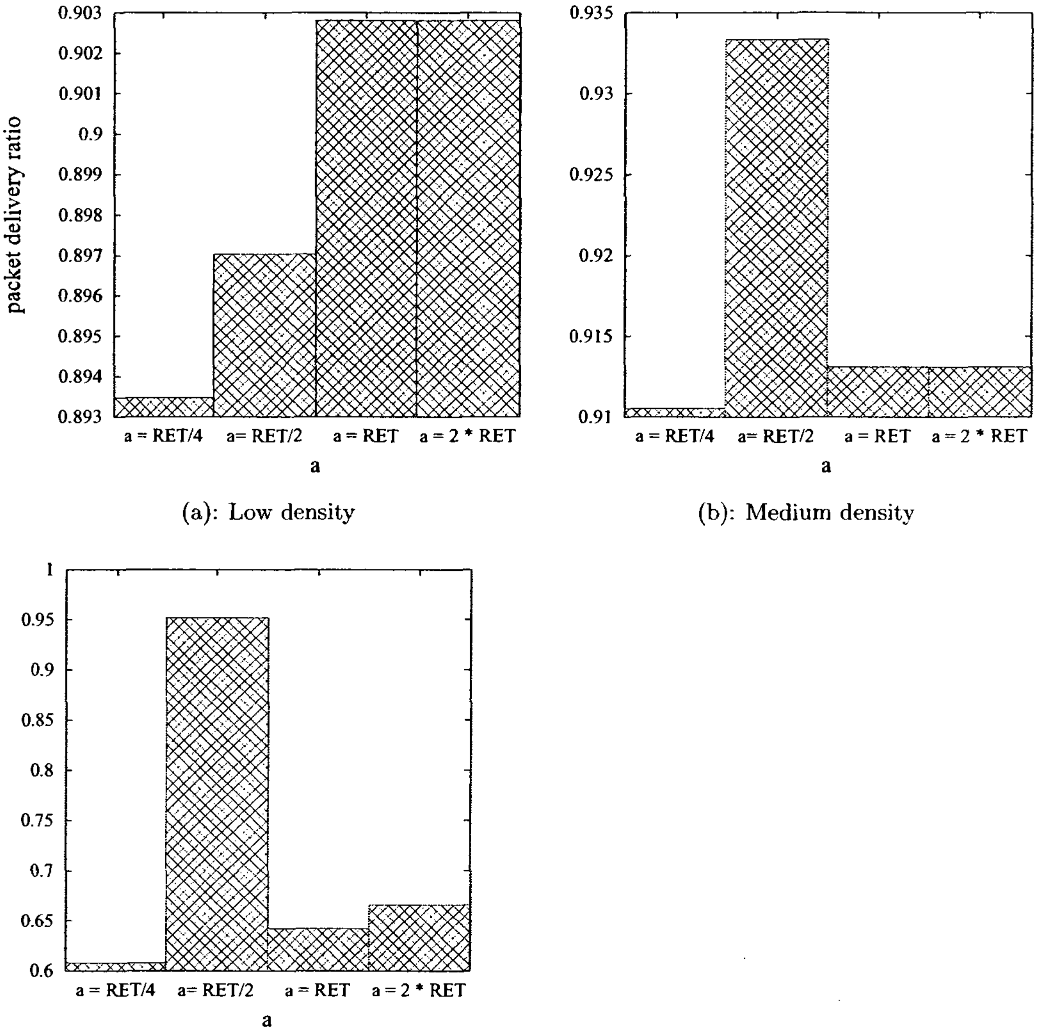
Figure 5.1(a) shows the packet delivery ratio goes up when we increase α, however, at a certain point it starts to fall down. The packet delivery ratio also drops sharply when we set α to 1. Indeed, as we put more weight on the stability, the selected routes become more stable and this increases the number of successful deliveries. However, NS2 trace files showed that when $\alpha = 1$, a large number of data packets are being dropped by the interface queue. The reason is that by giving all the weight to the stability, the number of duplications increases, as we discussed earlier. As the number of duplications reach a certain level, they flood the network, and this will overflow the interface queues after MAC layer, as observed from our simulations. On the other hand, as α increases, the delay increases mostly in the scenarios with large number of nodes. Putting more weight on stability make routes live longer, and when the node density is higher, the route travels through many hops (close to each other). In addition, since we have larger number of relays, there will be more time spent in forwarding packets and contending for accessing the medium, which makes the delay increase.

Figures 5.1(a) and 5.1(b) clearly show that if we choose $\alpha = 0.8$ most of the time we get the highest delivery rate with the lowest delay. So $\alpha = 0.8$ seems to be a good choice for our further simulations.

5.2.2 Evaluate our Selected Value for a

Now that we found a proper value for α, we will evaluate our suggested value for a. For this purpose, we evaluated 3 scenarios: Low density, Medium density and High density scenarios using $100, 200$ and 400 vehicles respectively. The maximum speed has been set to 30m/s, and we set a to different values $\frac{RET}{4}, \frac{RET}{2}, RET, 2 \times RET$, which means the LET values larger than $RET, 2 \times RET, 4 \times RET, 8 \times RET$ are being filtered respectively ($LET > 4 \times a$). Figure 5.2 illustrates the result of our simulations.

Figure 5.2(a) shows that in low density scenarios, if we set a to $\frac{RET}{2}$, the ratio of the delivered packets is less than larger values of a, this difference is less than 1% and is negligible. However, in the medium density and high density scenarios (figures 5.2(b) and 5.2(c))it can be seen that the suggested value shows higher packet delivery ratio than the other selected values. Specially in the high density scenario the



(a): Low density

(b): Medium density

(c): High density

Figure 5.2: Different values of a

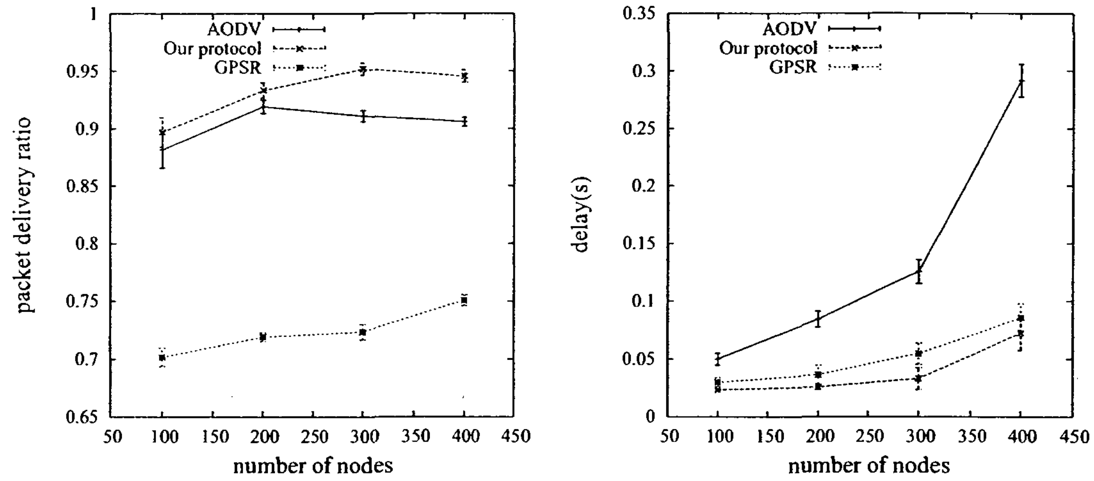
difference is noticeable, which is about 30%. As figure 4.6 shows, selecting different values of a changes the result of function S as shown in equation (4.6); the larger is the value of a the smoother the function grows. Besides, as explained earlier $4 \times a$ is the point beyond which the values of S are being filtered and they are considered to be equal in terms of stability, and the result of the ultimate function will be more dependent on the progress.

In low density scenarios since there are not many vehicles available, there is not much competition between vehicles for becoming the relay. Hence, changing the filtering point will not have much effect on the result. However, when the number of vehicles goes up, more vehicles compete to become the next relay, so the filtering point should be selected in a way that the best vehicle be selected for this purpose. Selecting large or low values of a will reduce the effect of the stability in the network, larger values will cause more duplication in the network and lower values will increase the role of progress and decrease the effect of stability of the links in the network.

5.2.3 Evaluation

To evaluate our protocol we performed some simulations with different node densities and speed. In all the scenarios we set α to be 0.8, and other parameters are set as explained earlier. To see the effect of changing the node densities on different protocols we fixed the maximum speed of vehicles to 30m/s and changed the number of vehicles on the road. To see the effect of changing the maximum speed, we fixed the number of vehicles on the road to 200.

We studied the effect of changing the speed and number of nodes on the packet delivery ratio and packet delivery delay on GPSR, AODV+ and our protocol. We then studied the effect of same changes on the overhead for our protocol and AODV+. We also changed the transmission range of the nodes and studied how it effects the packet delivery ratio and delay on our protocol and AODV+.



(a): Packet delivery ratio

(b): Packet delay

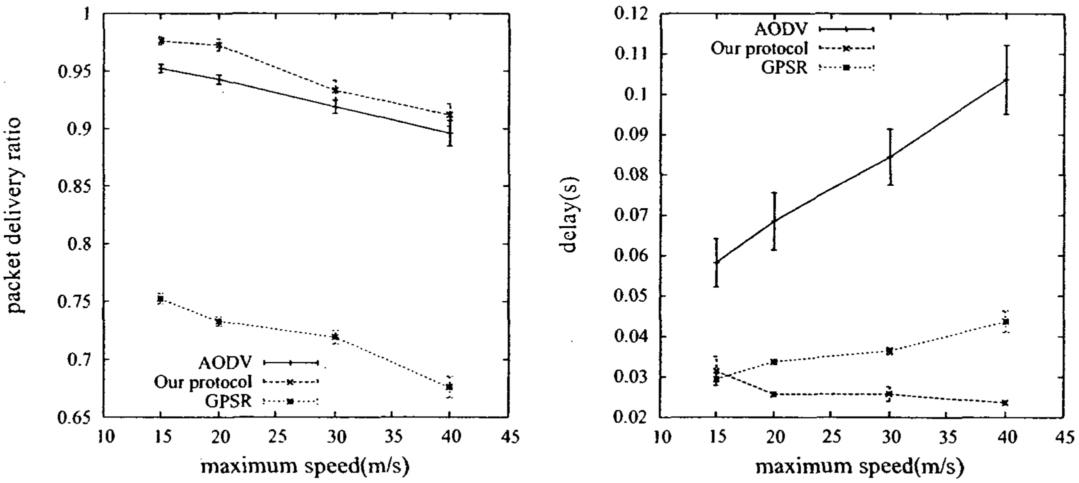
Figure 5.3: Varying number of nodes

Changing the Number of Nodes on the Road

By increasing the node density in the simulation, the delay slightly increases. This happens because the number of vehicles that may become a relay increases; therefore, there are more opportunities for building blocks of a route and routes may potentially become more stable. In addition, these routes can contain more hops. Hence, a vehicle can use a route that is more stable for a longer period than the scenarios with fewer vehicles, and this results in higher delivery delays as shown in figure 5.3(b). In addition, as the number of nodes increases, the probability that a vehicle has more than one route entry in its routing table increases. This increase in the stability of routes and connectivity in the network cause an increase in the packet delivery ratio as can be seen in figure 5.3(a).

Changing Maximum Speed of Vehicles

Figure 5.4 shows the results of varying the speed of vehicles. Increasing the speed will result in having links with smaller life-time and this leads to less stable routes. Indeed, these routes with small life-times cannot maintain a large number of hops.



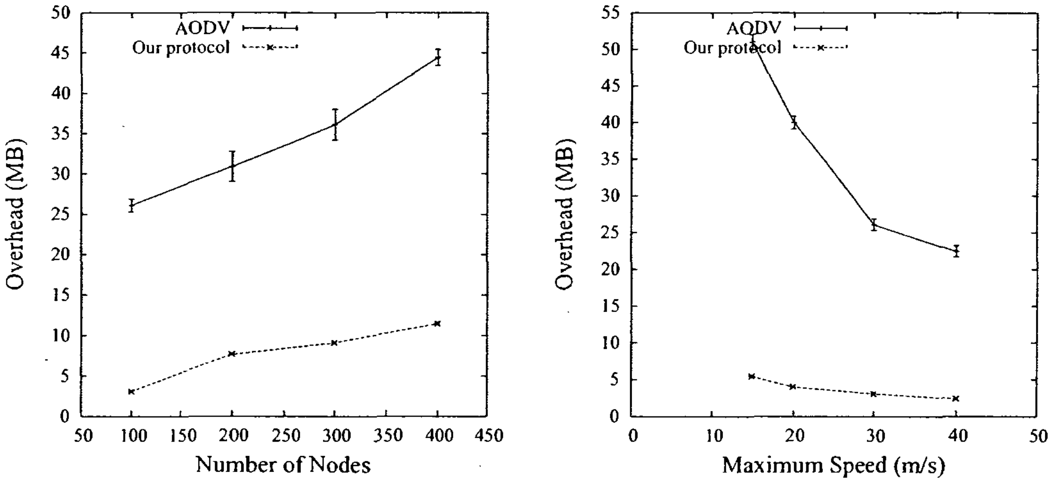
(a): Packet delivery ratio

(b): Packet delay

Figure 5.4: Varying maximum speed

Also the likelihood that a link fails unexpectedly increases, in this case, a packet might be dropped in the middle of the route since one of the relays may not be in the transmission range anymore. This decrease in the number of hops results in smaller delivery delays as shown in figure 5.4(b) (since less time is spent in contention for the medium), and the instability of routes will make the packet delivery ratio decrease (figure 5.4(a)).

AODV shows a good delivery ratio as figure 5.4(a) shows, however, the delay increases as vehicles move faster on the road. This is because if AODV cannot find a route to the destination, it buffers the packets until it finds a route to the destination or the related timer expires, in this case it can manage to finally find a way to the destination for the packets but the waiting time might be long. GPSR on the other hand does not show a good delivery ratio, but the delivery delay is acceptable. In GPSR nodes are forwarding the packet in a greedy manner; it means that the closest node to the destination in each step forwards the packet towards the destination. But due to the high speed of the vehicles, this relative closeness changes rapidly and is not true in a small portion of the time. It will cause routing problems for GPSR in



(a): Overhead by varying the number of nodes

(b): Overhead by varying the speed

Figure 5.5: Overhead comparison

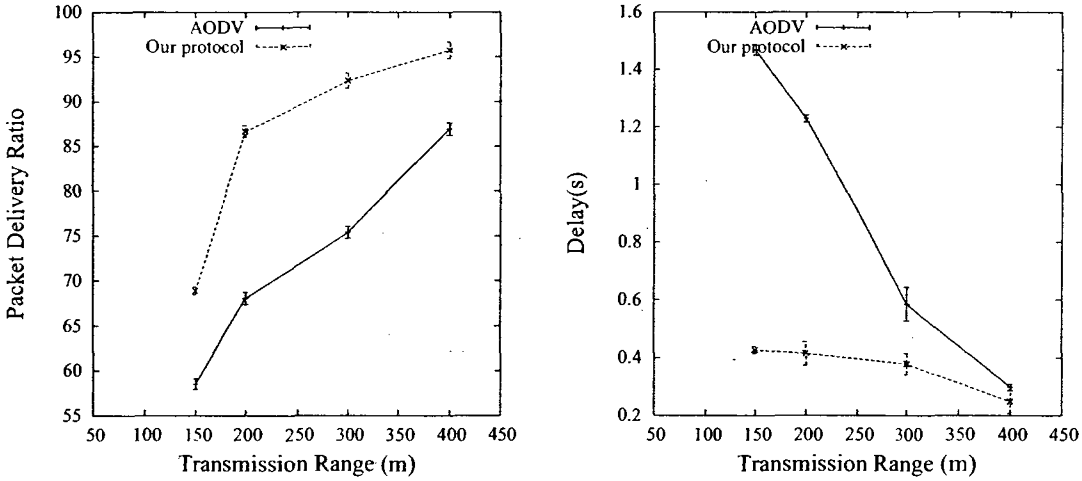
VANET scenarios, since GPSR is forwarding the messages based on the distance of nodes. However, those packets that find their way to the destination will be delivered in a timely manner, since the shortest path is being selected each time.

In both scenarios, GPSR and our suggested protocol have less delay than AODV. In AODV the route discovery process for the nodes outside the advertisement zone (which has been set to 3 hops here) will add a large delay to the packet delivery. Increasing the advertisement zone in this case will lead to higher overhead and probably network overflow. However, the packet delay for GPSR and our suggested protocol are close to each other. In our case, a vehicle already has a route to a gateway and forwarding a packet is as simple as a routing table lookup. Also in both scenarios, our suggested protocol performs better than both AODV and GPSR in the case of packet delivery ratio. In general our experiments show that our protocol performs better (in terms of packet delivery ratio and delay) than GPSR and AODV, under different network settings.

Studying the Overhead

Other than the packet delivery ratio and end to end delay, we decided to compare the overhead caused by our protocol with what is produced by AODV+. We did not compare it to GPSR since it uses a location based service other than the routing protocol and it requires to implement the location service in addition to the protocol itself. The result of this comparison is illustrated in figure 5.5. Figure 5.5(a) shows that by increasing the number of vehicles on the highway the overhead increases accordingly, both in AODV+ and our protocol. The reason is that as the number of nodes increases, in AODV+ more nodes are rebroadcasting the advertisement messages and this will cause more control messages to be transmitted in the network. In our protocol, more nodes means the advertisement messages have to be broadcast to more nodes than before, and it causes an increase in the number of control messages, and this increases the overhead. However, in our protocol this increase will not be as much as what happens in AODV+, since in AODV+ as mentioned earlier all the nodes that are located three hops away from the broadcaster node, will rebroadcast the message. In our protocol on the other hand, only one node is rebroadcasting the advertisement message, among the nodes who receive such a message.

Figure 5.5(b) shows the effect of increasing the maximum speed of vehicles on the total overhead. Increasing the maximum speed of vehicles on the road will decrease the overhead. As the speed of vehicles increases, they spend less time on the road during the simulation period. This means that the number of control messages that are transmitted in the same period of time decreases, and so the number of transmitted data messages. The number of transmitted control messages are dependent on the number of vehicles (both in AODV+ and in our protocol), so increasing the speed affects this number as the number of active nodes at each moment decreases, and will result in less overhead. The lower is the maximum speed of the vehicles on the road, the higher is the difference between the two protocols'



(a): Packet delivery ratio

(b): Packet delay

Figure 5.6: Evaluating by changing the transmission range of each node

overhead. Since in AODV+ all the nodes are actively take part in rebroadcasting the advertisement messages from gateways, the more time they spend in a zone of a gateway, they broadcast more and more advertisement messages from that gateway. On the other hand, in our protocol only selected nodes rebroadcast such messages, and changing the speed will not affect the overhead as much as it affects AODV+.

Figure 5.5 shows that our protocol produces less overhead than AODV+. As explained earlier, the reason is that in our protocol, only selected nodes (called relays) will rebroadcast the message in the network and the confined area (broadcast zones). However, in AODV+ all the vehicles that are receiving the advertisement messages will rebroadcast them into the network. The amount of overhead produced by AODV+ is on average 5 times that of our protocol.

Changing the Transmission Range

Another interesting parameter is the transmission range, we study the effect of changing the transmission range on our protocol. We simulated scenarios in which the number of the nodes on the road and the maximum speed is fixed to 200 nodes and

30m/s. Transmission range has been set to 150m, 200m, 300m and 400m in different scenarios and the results are presented in figure 5.6.

Figure 5.6(a) illustrates the effect of changing the transmission range on the packet delivery ratio. As it can be seen both AODV+ and our protocol behave in the same way, increasing the transmission range increases the packet delivery ratio. The reason is obvious, by increasing the transmission range, vehicles are getting covered by more gateways, and most of the multi-hop connections changes to single hop connection between the vehicle and the gateway. This increase in the number of direct connections in the network will improve the quality of the connection and more packets can be delivered using these direct connections. On the other hand, by increasing the transmission range the life-time of the links increases, since vehicles are spending more time in the transmission range of the gateways or each other. The longer the length of the connections, the less fragmentation occurs in the network. Besides that, when the transmission range reaches 400m, the gap between the coverage area of the gateways becomes only 100m and since vehicles now have bigger transmission ranges, they inform other vehicles about the existence of a gateway ahead a long time before vehicles exit the coverage area of the current gateway. The same story is true for ADOV+, since more direct connections and fewer broadcasts occur.

Figure 5.6(b) shows the effect of changing the transmission range on the packet delivery delay. Delay decreases as the transmission range increases. As explained earlier, since the number of direct connections increases, packets are being delivered faster than before. In addition in AODV+, more nodes are in the zone of a single node and the number of RREQ messages decreases rapidly, this will remove the route discovery time for most of the nodes and the delivery delay improves with a very fast pace. When we set the transmission range to 400m, AODV+ and our protocol are delivering the packets almost with the same delay. The reason is, that at this level most of the packets are being transmitted over single hop, or at most over a link with two hops and the routing protocol does not play an important role in determining the packet delay.

We performed some simulations and showed the effect of changing the transmission range on the packet delivery ratio and delivery delay. However, our scenario contained 200 nodes which is an average highway scenario. For future work, we will study the effect of transmission range on a busier highway (e.g with 1000 nodes). In this case, increasing the transmission range may have an inverse effect on the packet delivery ratio, due to number of the nodes. The interference and collisions might increase in that case and packet might be dropped or be delivered with greater delays than the scenarios with lower transmission range.

Chapter 6

Conclusion and Future Directions

6.1 Conclusion

Vehicular networks will become an important part of the vehicular electronics in the near future. These networks are trying to increase the safety on the road by informing the driver about the traffic conditions and different situations, before the vehicle reaches that point. Beside, safety application vehicular networks can be used for entertainment and information purposes such as Internet access. Internet access in the vehicles seem to be necessary as more people are getting tied to the Internet.

In this work we presented a novel scheme to connect vehicular networks to the Internet. This new scheme uses the vehicle movement parameters to predict the link stability of different nodes in order to create a more stable routes. We also introduced a new scheme for broadcasting the advertisement messages into the network based on Contention Based Forwarding (CBF), which tries to avoid broadcast storms in the network and decrease the overhead. In addition, our protocol tries to hand over the connections from one gateway to the other seamlessly by informing the vehicle about the existence of the gateways ahead before the vehicle leaves the coverage area of the current gateway. By using more stable routes, the amount of fragmentation in the network decreases and the network becomes more robust.

We also performed some exhaustive simulations to evaluate or work, and we presented the results in chapter 5. We compared our protocol with AODV and GPSR and we showed that our protocol performs better than these protocols in terms of packet delivery ratio, packet delivery delay and overhead. We also presented the effect of changing the transmission range of the nodes on our protocol.

6.2 Future Directions

Connecting vehicular networks to the Internet by using road infrastructure units requires that connection properties do not depend on the location of the vehicles. As explained earlier, IP address should be unique for each vehicle and as the vehicle moves, IP address should not be changed. Due to the large number of the vehicles on the road, IPv6 should be used to assign IP addresses to vehicles. In order to handle the vehicle mobility, Mobile IPv6 can be used. In future works, we plan to integrate our work with Mobile IPv6 in order to handle the mobility.

Current work is trying to introduce a novel way to connect vehicular networks to the Internet by finding and selecting the most stable routes. However, selecting relays based only on the life-time of the links may cause bottlenecks, and some potentially good routes can be left undiscovered. It might happen when the number of nodes on the road is high, one vehicle might become the relay due to its link stability for many vehicles during a time period. In this case, the traffic on one link increases and packet drops occurs over the shared link. To overcome these limitations, some probabilistic methods will be added to our work in order to make better route selections to satisfy the Quality of Service (QOS) requirements. For instance, as the number of connected vehicles to a node increases the probability that it rebroadcasts the advertisement messages decreases, and another node with less stable link and more bandwidth available will play the relay role.

Besides, we introduced some approaches to omit the inevitable message duplications as much as possible, however further improvements should be applied in this area. In our future work, we are going to measure the duplications and suggest better approaches to reduce the number of duplications as much as possible.

Another issue relates to the data rate with which vehicles are communicating with the roadside infrastructure units. In our protocol we assumed that vehicles are transmitting data to the gateway at the same rate. However, this assumption is too simple and is not true. The communication rate is related to the communication distance between the moving vehicle and gateway. In our future works we are going to use a rate adaptation scheme in order to evaluate our protocol better.

Security issues should be studied as well. Different vulnerabilities and possible attacks should be considered, and possible solutions to these problems should be discussed as well.

Bibliography

[1] "Transport canada. http://www.tc.gc.ca."

[2] "Mobile ad-hoc networks(manet) http://www.ietf.org/html.charters/manet-charter.html."

[3] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *Communications Magazine, IEEE*, vol. 40, no. 8, pp. 102–114, 2002.

[4] W. Kiess, J. Rybicki, and M. Mauve, "On the nature of inter-vehicle communication," *4th Workshop on Mobile Ad-Hoc Networks*, 2007.

[5] "Gsm, global system for mobile communications. http://www.gsm.org."

[6] "Umts, universal mobile telecommunications system. http://www.umtstdd.org/."

[7] "Imt-2000, international telecommunication union. http://www.itu.int/osg/spu/imt-2000/technology.html."

[8] "Ieee 802.11x standards. http://grouper.ieee.org/groups/802/11/."

[9] "Standard specification for telecommunications and information exchange between roadside and vehicle systems - 5 ghz band dedicated short range communications (dsrc) medium access control (mac) and physical layer (phy) specifications," Sept, 2003.

[10] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing Vehicular Communications - Assumptions, Requirements, and Principles," in *Workshop on Embedded Security in Cars (ESCAR) 2006*, 2006, pp. 5–14. [Online]. Available: http://www.escar.info/06/general.html

[11] C. E. Perkins and D. B. Johnson, "Mobility support in ipv6," in *Mobile Computing and Networking*, 1996, pp. 27–37. [Online]. Available: citeseer.ist.psu.edu/perkins96mobility.html

[12] C. Perkins *et al.*, "IP mobility support," 1996.

[13] H. Fler, M. Ksemann, M. Mauve, H. Hartenstein, and J. Widmer, "Contention-based forwarding for mobile ad-hoc networks," *Elsevier's Ad Hoc Networks*, vol. 1, no. 4, pp. 351 – 369, 2003.

[14] C. Perkins, "Ad-hoc on demand distance vector routing (aodv). internet-draft, november 1997. draft-ietf-manet-aodv-00.txt."

[15] G. Caizzone, W. Erangoli, P. Giacomazzi, and G. Verticale, "An enhanced gpsr routing algorithm for tdma-based ad-hoc networks," *IEEE GLOBECOM '05.*, Nov.-2 Dec. 2005.

[16] S. Kumar, V. S. Raghavan, and J. Deng, "Medium access control protocols for ad hoc wireless networks: A survey," *Ad Hoc Networks*, vol. 4, no. 3, pp. 326 – 358, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/B7576-4DPGSVH-1/2/58c0f2f528f8d27ecd834b2e92c21515

[17] C. D. M. Cordeiro and D. P. Agrawal, "Mobile ad hoc networking," *Center for Distributed and Mobile Computing, ECECS, University of Cincinnati*, 2003.

[18] R. Ramanathan, J. Redi, and B. Technologies, "A brief overview of ad hoc networks: challenges and directions," *IEEE Communications Magazine*, vol. 40, no. 5, pp. 20–22, 2002.

[19] M. Scott Corson, J. Macker, and S. Batsell, "Architectural considerations for mobile mesh networking," *Military Communications Conference, 1996. MILCOM '96, Conference Proceedings, IEEE*, vol. 1, pp. 225–229 vol.1, Oct 1996.

[20] M. Mauve, A. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *IEEE network*, vol. 15, no. 6, pp. 30–39, 2001.

[21] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," *ACM SIGCOMM Computer Communication Review*, vol. 24, no. 4, pp. 234–244, 1994.

[22] S. Murthy and J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," *Mobile Networks and Applications*, vol. 1, no. 2, pp. 183–197, 1996.

[23] D. Johnson, D. Maltz, J. Broch *et al.*, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad hoc networking*, vol. 5, pp. 139–172, 2001.

[24] C. Perkins, E. Belding-Royer, S. Das *et al.*, "Ad hoc on-demand distance vector (AODV) routing," 2003.

[25] Z. Haas, M. Pearlman, and P. Samar, "The zone routing protocol (ZRP) for ad hoc networks," *TERNET DRAFT-Mobile Ad hoc Networking (MANET) Working Group of the bternet Engineering Task Force (ETF), November*, 1997.

[26] J. C. Navas and T. Imielinski, "Geocast—geographic addressing and routing," in *MobiCom '97: Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking.* New York, NY, USA: ACM, 1997, pp. 66–76.

[27] R. Jain, A. Puri, and R. Sengupta, "Geographical routing using partial information for wireless ad hoc networks," *IEEE Personal Communications*, vol. 8, pp. 48–57, 2001.

[28] R. Morris, A. C. Smith, A. H. Routing, J. Li, and J. Li, "A scalable location service for geographic ad hoc routing," in *AdHocRouting,intheProceedings of the 6th ACM International Conference on Mobile Computing and Networking (MobiCom '00*, 2000, pp. 120–130.

[29] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, "A distance routing effect algorithm for mobility (dream)," in *MobiCom '98: Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking.* New York, NY, USA: ACM, 1998, pp. 76–84.

[30] Y. Ko and N. Vaidya, "Location-Aided Routing (LAR) in mobile ad hoc networks," *Wireless Networks*, vol. 6, no. 4, pp. 307–321, 2000.

[31] T. Camp, "Location information services in mobile ad hoc networks," in *In Proceedings of the IEEE International Conference on Communications (ICC*, 2002, pp. 3318–3324.

[32] S. Giordano, I. Stojmenovic, and L. Blazevic, "Position based routing algorithms for ad hoc networks: A taxonomy," *Ad Hoc Wireless Networking*, pp. 103–136, 2004.

[33] I. Stojmenovic, "Position-based routing in ad hoc networks," *Communications Magazine, IEEE*, vol. 40, no. 7, pp. 128–134, Jul 2002.

[34] H. Takagi and L. Kleinrock, "Optimal transmission ranges for randomly distributed packet radio terminals," *Communications, IEEE Transactions on*, vol. 32, no. 3, pp. 246–257, Mar 1984.

[35] E. Kranakis, S. O. C. Science, H. Singh, and J. Urrutia, "Compass routing on geometric networks," in *in Proc. 11 th Canadian Conference on Computational Geometry*, 1999, pp. 51–54.

[36] B. Karp and H. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking.* ACM New York, NY, USA, 2000, pp. 243–254.

[37] C. Perkins, S. Alpert, and B. Woolf, *Mobile IP; Design Principles and Practices.* Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA, 1997.

[38] H. Ammari, "A survey of current architectures for connecting wireless mobile ad hoc networks to the Internet," *International Journal of Communication Systems*, vol. 20, no. 8, 2007.

[39] H. Soliman, C. C. K. Malki, and L. Bellier, "Hierarchical mipv6 mobility management," October 2002.

[40] R. Koodli *et al.*, "Fast handovers for mobile IPv6," 2003.

[41] H. Soliman, C. C. K. Malki, and L. Bellier, "Simultaneous bindings for mobile ipv6 fast handoffs," June 2002.

[42] R. Hsieh, Z. Zhou, and A. Seneviratne, "S-mip: a seamless handoff architecture for mobile ip," *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, vol. 3, pp. 1774–1784 vol.3, 30 March-3 April 2003.

[43] M. Corson, J. Macker, and G. Cirincione, "Internet-based mobile ad hoc networking," *IEEE Internet Computing*, vol. 3, no. 4, pp. 63–70, 1999.

[44] H. M. Ammari, "A survey of current architectures for connecting wireless mobile ad hoc networks to the internet," *International Journal of Communication Systems*, vol. 20, no. 8, pp. 943–968, 2007.

[45] U. Jönsson, F. Alriksson, T. Larsson, P. Johansson, and J. Gerald Q. Maguire, "Mipmanet: mobile ip for mobile ad hoc networks," in *MobiHoc '00: Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing.* Piscataway, NJ, USA: IEEE Press, 2000, pp. 75–85.

[46] Y. Sun, E. Belding-Royer, and C. Perkins, "Internet connectivity for ad hoc mobile networks," *International Journal of Wireless Information Networks*, vol. 9, no. 2, pp. 75–88, 2002.

[47] H. Ammari, "Using group mobility and multihomed mobile gateways to connect mobile ad hoc networks to the global IP Internet," *International Journal of Communication Systems*, vol. 19, no. 10, 2006.

[48] W. Enkelmann, "Fleetnet - applications for inter-vehicle communication," *Intelligent Vehicles Symposium, 2003. Proceedings. IEEE*, pp. 162–167, June 2003.

[49] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking.* New York, NY, USA: ACM, 1999, pp. 151–162.

[50] Q. Xu, R. Segupta, D. Jiang, and D. Chrysler, "Design and analysis of highway safety communication protocol in 5.9 ghz dedicated short range communication spectrum," in *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*, vol. 4, 2003.

[51] A. Benslimane, "Optimized dissemination of alarm messages in vehicular ad-hoc networks (vanet)," *7th IEEE Int. Conf. HSNMC*, vol. LCNS 3079, pp. 655–666, 2004.

[52] S. Jaap, M. Bechler, and L. Wolf, "Evaluation of routing protocols for vehicular ad hoc networks in city traffic scenarios," in *International Conference on Intelligent Transportation Systems Telecommunication (ITST), Brest, France*, 2005.

[53] H. Füßler, M. Mauve, H. Hartenstein, M. Käsemann, and D. Vollmer, "A comparison of routing strategies for vehicular ad hoc networks," *Department of Computer Science, University of Mannheim, Tech. Rep. TR-02-003*, 2002.

[54] C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments," in *IEEE Intelligent Vehicles Symposium, 2003. Proceedings*, 2003, pp. 156–161.

[55] J. Tian, L. Han, and K. Rothermel, "Spatially aware packet routing for mobile ad hoc inter-vehicle radio networks," *Intelligent Transportation Systems, 2003. Proceedings. 2003 IEEE*, vol. 2, pp. 1546–1551 vol.2, 12-15 Oct. 2003.

[56] J. Chennikara-Varghese, W. Chen, O. Altintas, and S. Cai, "Survey of routing protocols for inter-vehicle communications," in *The Second International Workshop on Vehicle-to-Vehicle Communications*, 2006.

[57] H. Füßler, H. Hartenstein, J. Widmer, M. Mauve, and W. Effelsberg, "Contention-based forwarding for street scenarios," in *1st International Workshop in Intelligent Transportation (WIT 2004)*, 2004.

[58] P. Kumar, J. Kuri, P. Nuggehalli, M. Strasser, M. May, and B. Plattner, "Connectivity-aware routing in sensor networks," *Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on*, pp. 387–392, 14-20 Oct. 2007.

[59] V. Naumov, R. Baumann, and T. Gross, "An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces," in *Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing.* ACM New York, NY, USA, 2006, pp. 108–119.

[60] W. Sun, H. Yamaguchi, K. Yukimasa, and S. Kusumoto, "Gvgrid: A qos routing protocol for vehicular ad hoc networks," *Quality of Service, 2006. IWQoS 2006. 14th IEEE International Workshop on*, pp. 130–139, June 2006.

[61] H. Menouar, M. Lenardi, and F. Filali, "Movement prediction-based routing (mopr) concept for position-based routing in vehicular networks," *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, pp. 2101–2105, 30 2007-Oct. 3 2007.

[62] H. Menouar, M. Lenardi, F. Filali, H. Eur, and S. Antipolis, "Improving Proactive Routing in VANETs with the MOPR Movement Prediction Framework," in *Telecommunications, 2007. ITST'07. 7th International Conference on ITS*, 2007, pp. 1–6.

[63] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications*, vol. 13, no. 5, p. 8, 2006.

[64] M. Gerlach, "VaneSe-An approach to VANET security," *Proceedings of the V2VCOM*, 2005.

[65] J. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, 2004.

[66] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proceedings of HotNets-IV*, 2005.

[67] M. Raya, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks.* ACM New York, NY, USA, 2005, pp. 11–21.

[68] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *European Wireless*, 2002, pp. 270–274.

[69] "The fleetnet project. http://www.ct2.tu-harburg.de/fleetnet/english/documents.html."

[70] M. Bechler, L. Wolf, O. Storz, and W. Franz, "Efficient discovery of internet gateways in future vehicular communication systems," *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*, vol. 2, pp. 965–969 vol.2, 22-25 April 2003.

[71] M. Bai, L. Wolf, and W. Franz, "Mobile internet access in fleetnet," *13. Fachtagung Kommunikation in verteilten Systemen KiVS 2003*, February 2003.

[72] R. Baldessari, A. Festag, and J. Abeille, "NEMO meets VANET: a deployability analysis of network mobility in vehicular communication," in *Telecommunications, 2007. ITST'07. 7th International Conference on ITS*, 2007, pp. 1–6.

[73] G. Korkmaz, E. Ekici, and F. Ozguner, "Internet access protocol providing qos in vehicular networks with infrastructure support," *Intelligent Transportation Systems Conference, 2006. ITSC '06. IEEE*, pp. 1412–1417, Sept. 2006.

[74] V. Namboodiri, M. Agarwal, and L. Gao, "A study on the feasibility of mobile gateways for vehicular ad-hoc networks," 2004. [Online]. Available: citeseer.ist.psu.edu/namboodiri04study.html

[75] C. Sommer and F. Dressler, "The dymo routing protocol in vanet scenarios," *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, pp. 16–20, 30 2007-Oct. 3 2007.

[76] I. Chakeres and C. Perkins, "Dynamic MANET on-demand (DYMO) routing," *draft-ietf-manet-dymo-03. txt, Internet Draft (work in progress)*, 2005.

[77] M. Bechler and L. Wolf, "Mobility management for vehicular ad hoc networks," *Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st*, vol. 4, pp. 2294–2298 Vol. 4, 30 May-1 June 2005.

[78] W. Su, S.-J. Lee, and M. Gerla, "Mobility prediction and routing in ad hoc wireless networks," *International Journal of Network Management*, vol. 11, no. 1, pp. 3 – 30, 2001.

[79] "The network simulator - ns-2. http://www.isi.edu/nsnam/ns/."

[80] U. Korner, A. Hamidian, and A. Nilsson, "Performance of internet access solutions in mobile ad hoc networks," *Dagstuhl-Workshop "mobility and Wireless in Euro-NGI"*, pp. 189–201, 2005.

[81] "Rapid generation of realistic simulation for vanet. http://lens1.csie.ncku.edu.tw/move/index.htm."

[82] "SUMO - Simulation of Urban MObility http://sumo.sourceforge.net/."