Chapter 3

Project: Seamless roaming (mobile-home, mobile-office)

3.1 Introduction

In this Chapter we will describe the Project "*Seamless roaming (mobile-home, mobile-office)*", developed from November 2006 to March 2008, in collaboration with University of Rome "Sapienza", University of Rome "Tor Vergata", and Telecom Italia Mobile (TiLab, Turin).

This project has focused on the study and design of advanced techniques for mobility and connectivity management in heterogeneous network scenarios, where users move and need to be always connected. (*i.e.* from home to office, and vice versa).

Collaborative frameworks support joint work for a team of people in a number of possible application scenarios. A useful feature to support is interworking of teams of participants from different remote networks (*i.e.* home, office, malls, theaters, etc.).

A middle-ware layer is then generally required in order to allow secure and high-quality

interconnection of remote network sites supporting a distributed service environment. For example, a typical e-health scenario [47] includes collaborative services for virtual health-care teams (doctors, patients, care team and pharmacy), including telemedicine, management of electronic medical records and automatic diagnosis systems.

Health-care professionals share information on patients through digital equipments and interact with each other and with the patient as in the same physical place, though they might be actually distributed in different remote sites, *i.e.* patient's or health-care professional's LAN (Local Area Network).

In a typical service scenario, a body sensor network can be deployed in order to monitor a patient, who is aided by a nurse in her or his home environment and is interconnected with a team of doctors who reside in remote sites.

Another context in which a collaborative framework can be exploited is a disaster recovery scenario [48], in which, after a flood or an earthquake, the network infrastructure and relevant services become unavailable. In order to rescue people, civil protection teams need to quickly set-up network links and provide various services, including basic communication, environmental monitoring, and medical services.

In both scenarios, a virtual network infrastructure is necessary to interconnect each network site and provide service management facilities including service discovery, presentation, access and control. The target infrastructure should be able to add or remove service components automatically and satisfy e-health or disaster service requirements.

Basically, doctors or civil protection operators do not have the skills to configure new networks including body or environmental sensors and to enable service discovery mecha-

nisms. Hence, autonomy and self-configuration capabilities are key features of the technologies to adopt for the collaboration framework, which should assure minimal intervention by the end users.

Service discovery is an important feature for management of a service network. It is responsible for detecting new devices and service instances when they come into communication range or leave the environment.

With policy-driven mechanisms, service discovery can be easily adapted to different applications and support self configuration features. In a typical service discovery architecture, requests to discover new components are periodically broadcast. In turn, any discoverable component can share its own services by sending a message which includes synthetic information on the provided services and how to access them such as its identifier, network address (or domain name), device type and list of offered services.

The device can then be queried to obtain its complete profile, which describes the characteristics of the services it provides, any credentials it offers along with other potentially useful information. In general, each component has its own policies specifying how to respond to discovery requests.

In this Chapter we will describe a novel efficient and reliable intranet, combining the concept of VPN (Virtual Private Network) remote access with local resources and service discovery, based on UPnP extension with the open source OpenVPN [49, 50] framework.

This is based on a model, *i.e.* "Tunneling with Service Discovery", for accessing local services from a remote network. The model enables the interworking of multiple networks so that users can transparently access the advertised services in any of the networks as if

they were local services provided within a single physical network. The model also allows One-way Access, Multi-Network Access and Multi-Stage Access with a simplified network configuration.

3.2 UPnP Standard

Home network is started for share of resources, remote education, remote treatment, home automation, and multimedia services at home (see Figure 3.1). An effective middleware is needed to control the home appliances regardless of home network and sensor technologies applied, like ZigBee (IEEE 802.15.4) and the UPnP (Universal Plug and Play).

Figure 3.1: Home network.

The emerging protocol UPnP [51] for device/service discovery and control can be ex-

ploited to build a collaborative framework in a Local Area Network. For example, on-body and environmental sensors are largely used for conveniently monitoring patients in emergency environment, by UPnP self configuration features. UPnP technology allows patients or medical personnel without technological expertise to deploy a self adaptive body-area network.

The UPnP extends the plug and play concept to the networking based on the standard Internet Protocol. The UPnP is an architecture for pervasive peer-to-peer network connectivity of intelligent appliances, wireless devices, and PCs. UPnP is a distributed, open networking architecture that leverages TCP/IP and the Web technologies to enable seamless proximity networking.

However, though UPnP is able to quickly establish a local network, it provides no support for conveniently and securely integrate a local service network to external networks, and enable exporting of service discovery out of a LAN. This issue represents the main aspect discussed in this Chapter. Our focus is to enlarge UPnP context and to extend its service discovery and control capabilities to a WAN (Wide Area Network) scenario, where multiple UPnP networks are interconnected into a reliable intranet.

3.3 UPNP extension with OpenVPN

A fundamental element for supporting UPnP WAN extension is the Residential Gateway (RG). The RG is typically a "zero-admin system", which is secure and functions as a gateway between local and remote networks.

Remote access technologies, such as Virtual Private Networks (VPNs) [52], are widely

used to access a remote local area network through Internet. VPN realizes a virtual local network across multiple physical networks. Various frameworks can be used to realize a VPN, including JXTA [53, 54], OSGi [55, 56], OpenVPN [49, 50], in addition to solutions based directly on IPSec [57].

OpenVPN [49, 50] is a free and open source Virtual Private Network (VPN) program for creating point-to-point or server-to-multiclient encrypted tunnels between host computers. It is able to establish direct links between computers across Network Address Translators (NATs) [58] and firewalls. As a matter, NATs and firewalls have spread through Internet, and most local-area networks has become not accessible directly from a remote network.

The choice to use OpenVPN is because it is particularly easy to install and robust for deployment of an overlay network across multiple networks.

It allows to pass through firewalls and has bridging features to establish an overlay network using Ethernet interfaces. It is a full-featured Secure Sockets Layer (SSL) VPN-based solution which can accommodate a wide range of configurations, including remote access, site-to-site VPNs, Wi-Fi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls. It implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or 2-factor authentication.

OpenVPN also allows user or group-specific access control policies, using firewall rules applied to the VPN virtual interface.

3.3.1 Proposed architecture

Our goal is to offer a model to extend UPnP service environment from a single LAN to multiple LANs (Figure 3.2). As a solution, we have joined distinct UPnP LANs with tunneling mechanisms provided by OpenVPN. Using UPnP is it possible to automatically maintain a list of services in a local network, which is regularly updated by service discovery. OpenVPN establishes IP tunnel across multiple physical LANs which are then interconnected into a single virtual LAN where any host can discover and access all the available services in any other hosts in the physical LANs, *i.e.* UPnP VPN (UVPN).

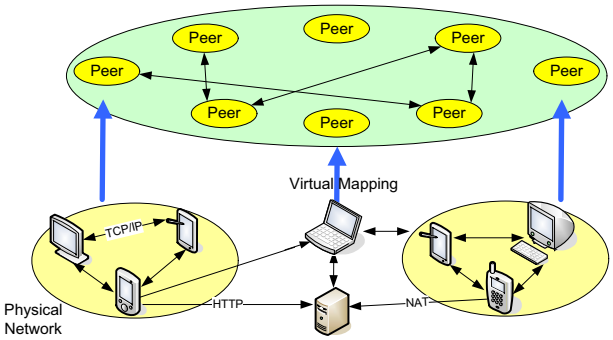


Figure 3.2: Virtual UPnP LAN on multiple physical LANs.

An OpenVPN tunnel (Figure 3.3) make it possible to relay traffic, either for service discovery and control signalling or for data packets, between two LANs. Namely, a tunnel propagates all traffic by means of specific relay agents placed at both ends of the tunnel, *i.e.* the OpenVPN server and the OpenVPN client, which enable communication between nodes in distinct LANs without the internal addressing architecture of each LAN being disclosed.

The OpenVPN server (Figure 3.4) realizes the RG (Residential Gateway) in our model,

as it provides access to services in a local network to remote nodes from another network. An OpenVPN client (Figure 3.4) in a local UPnP network uses the network address of a OpenVPN server in a remote UPnP network to create a tunnel entry point for each service available in the remote UPnP network.

In turn, the OpenVPN client advertises the available remote services to its local network using UPnP service discovery. Hence, the advertised services look like local services offered by the OpenVPN client to hosts within the client's local network, and thus, the hosts can access the services transparently without noticing that they are actually provided from a remote network through the OpenVPN client. From the point of view of a host providing a service, a service request from a remote network looks as coming from the OpenVPN server in the same local network since it is relayed from the remote OpenVPN client to the local OpenVPN server before reaching the host.

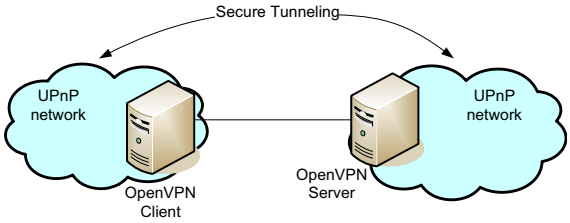


Figure 3.3: Secure Tunneling between UPnP networks with OpenVPN.

3.4 Test-bed Description

We set up a test environment in order to validate the architecture presented in Section 3.3. Namely, the NAT transversal capability of OpenVPN was demonstrated in order to fully support UPnP signaling across multiple networks. UPnP services were managed using

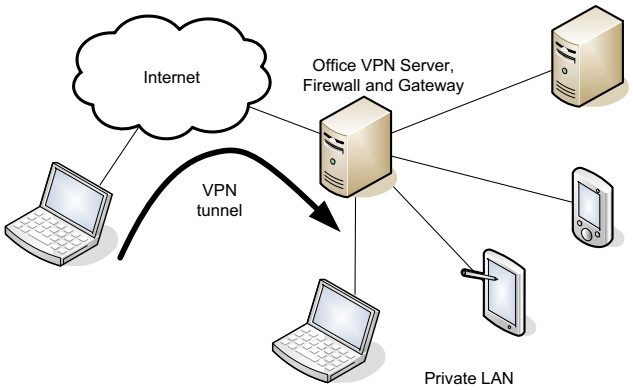


Figure 3.4: Remote access to a UPnP network with OpenVPN.

UPnP Intel Tools [59, 60].

The basic configuration which was used included the following network UPnP-enabled nodes:

- two laptops (LP 1 and LP 2) with Wi-Fi interfaces;
- an Access Point (AP) with Wi-Fi, and Ethernet interfaces;
- a Residential Gateway (RG) with Ethernet, and ADSL interfaces;
- a tablet PC with an ADSL interface;
- a PDA (Personal Digital Assistant) with GPRS/UMTS interfaces.

For implementing tunneling mechanisms, we set up a point to point connection with SSL/TLS adopting TAP 1 virtual interfaces that allow the exchange of encrypted packets in broadcast mode (essential for UPnP operation) and the establishment of point-to-point connection between client and server.

To secure the wireless network link between the OpenVPN client and server we built a

full PKI (Public Key Infrastructure). This infrastructure is very scalable and flexible. The servers and all clients must trust a single CA (Certification Authority). All keys/certificates which are rooted at this CA are used to negotiate and validate a TLS connection channel. Separate random session keys are negotiated over this channel and used for the tunnel.

The implemented testbed environment is depicted in Figure 3.5. It includes a local Wi-Fi area interconnected using two external networks via ADSL and UMTS links. LP1 and LP2 belong to the same physical IEEE 802.11 network. They have been configured as UPnP-enabled nodes and include a UPnP Media Server [61] device storing multimedia contents. They are interconnected by means of the access point.

Secure Internet access is provided through the RG node running an OpenVPN Server, which enables the interworking with remote OpenVPN clients. The Tablet PC and PDA are UPnP-enabled devices including AV Media Renderers [61] devices for playing multimedia files. They are able to communicate with the LAN area from two external networks, *i.e.* ADSL and UMTS respectively and have an OpenVPN client running. By virtue of OpenVPN, the UPnP service discovery messages generated by all these nodes can propagate beyond the LAN area and reach the other physical networks.

It is worth noticing that in Figure 3.5, the RG, the PDA and the Tablet PC have a network address of the same subnet `10.3.0.xxx`. These are not the actual public addresses of the nodes, they are rather used to identify the end-points of the tunnels of the OpenVPN overlay network. This scenario can be regarded as representative of a user with UPnP devices located in a local area and controlling them remotely while on the move (using a PDA as client) or from a remote office (using a Tablet PC as client).

We tested remote control of UPnP devices through Tablet PC and PDA. We first verified that both UPnP service discovery and service export propagated in the extended network area as if in a single LAN. Afterwards, we tested UPnP remote service access through Tablet PC and PDA. Namely, Tablet PC and PDA discovered the multimedia files in LP1 and LP2 and established a connection to the WLAN area to play the discovered contents remotely in streaming mode. Therefore, Tablet PC and PDA located in two external networks were able to discover, remotely control and use the services inside the virtual LAN area as if all nodes were in the same physical network. In this sense, we were able to prove that using OpenVPN, we effectively realized an UVPN (UPnP Virtual Private Network), which extended the scope of the services located in separate UPnP networks in the Internet.

Future work is focusing on the development and testing of a vertical policy-based handoff mechanism (Figure 3.6), driven by parameters such as RSSI (Received Signal Strength Indication), Quality-of-Service (QoS) parameters such as throughput, delay, jitter, packet loss probability) or monetary cost for streaming services. The vertical handoff scenario occurring in an UVPN is represented in Figure 3.6.

We have proposed a technological solution to implement a collaborative framework which can support virtual team environments in the context of various application domains, such as e-health or disaster recovery virtual teams. In order to realize a network infrastructure for collaborative work, we have selected two main reference technologies, *i.e.* UPnP and OpenVPN. UPnP allows convenient discovery, access and control of resources and services in a network. However, its operation is currently limited to a LAN environment as it extensively use broadcast of signaling. OpenVPN makes it possible to interconnect

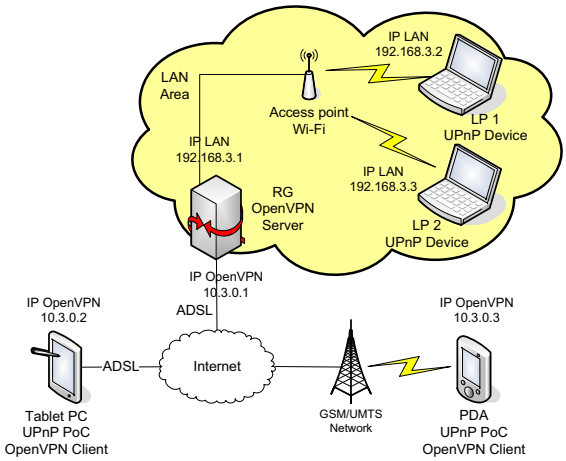


Figure 3.5: Testbed scenario: UPnP devices communication across heterogeneous access networks.

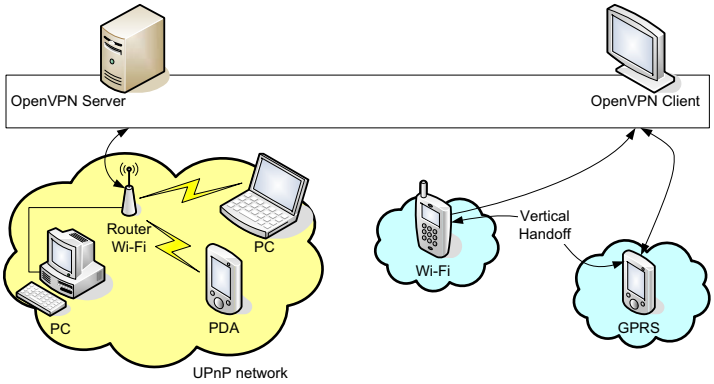


Figure 3.6: Vertical handoff in a UVPN scenario.

multiple UPnP networks in a single virtual LAN environment through IP tunnels and realize UVPN. In this work, we have proposed a reference architecture using UPnP and OpenVPN and validated it with a testbed environment realizing a UVPN. Namely, with our prototype we have demonstrated OpenVPN capability to transverse NAT/gateway in remote LANs and support UPnP signaling over a large heterogeneous virtual LAN.

Chapter 4

VANETs

4.1 Introduction

In this Chapter 4, we will describe the main behavior and characteristics of Vehicular Ad Hoc NETworks (VANETs), and which are the main open issues in such research theme.

Mobility and connectivity management in VANETs represent novel challenging problems, due to variable and random nature of such networks. Speed and different vehicles' densities cause disconnection periods, where vehicles are not able to communicate between them.

Vehicle-to-Vehicle (V2V), and Vehicle-to-Infrastructure (V2I) are the main two protocols for communications in VANETs. Each of them presents pro and contro, due to main aspects, like vehicles density, speed, infrastructure network topology, kind of technologies available on vehicles, and so on.

After depicting how VANETs work (Section 4.2), the IEEE 802.11p standard employed for vehicle-to-vehicle communications (Section 4.3), the protocols V2V and V2I, and the behaviour of VANETs as Delay Tolerant Networks (Section 4.4), in Section 4.5 we address

on a novel communication protocol which opportunistically exploits both V2V and V2I. It is called as V2X [7] that means a vehicle can be connected both via V2V and V2I, according to a switching protocol decision, (Subsection 4.5.1).

We show by simulation results that V2V is well employed in dense traffic scenarios, while V2I is preferred to V2V in sparse traffic scenarios.

Moreover, the V2X protocol is based on local information, that is forwarded in the VANET via multihop and gives the knowledge of traffic density. Then, particular vehicles equipped with traditional cellular and wireless network interface cards (*i.e.* UMTS, HSDPA, Wi-Fi, WiMAX, etc.) are able to be directly connected to Access Point or Base Stations (generally called as Road Side Units) displaced near the roads. The information of neighboring Road Side Units is obtained by the Infrastructure Connectivity parameter.

The effectiveness of V2X is also described by an improvement of message propagation rates. In Section 4.6 we will deal with a novel solution for opportunistic forwarding networking applied in VANETs. After defining the minimum and maximum bounds for message propagation rates in Section 4.7, we illustrate a novel message propagation algorithm based on V2X protocol in Subsection 4.7.1. In Subsection 4.7.2 simulation results are compared, with respect to traditional opportunistic networking adopted in VANETs, [62].

Finally, in Section 4.8 we briefly introduce a novel satellite-based service for safety applications in VANETs. More details are described in [9].

4.2 Vehicular Ad Hoc NETworks

Vehicular communication is considered as an enabler for driverless cars of the future [63]. Presently, there is a strong need to enable vehicular communication for applications such as safety messaging, traffic and congestion monitoring and general purpose Internet access.

VANETs is a term used to describe the spontaneous ad hoc network formed over vehicles moving on the roadway. Vehicular networks are fast emerging for developing and deploying new and traditional applications.

VANETs are characterized by high mobility, rapidly changing topology, and ephemeral, one-time interactions. Applications such as safety messaging are near-space applications where vehicles in close proximity, typically of the order of few meters, exchange status information to increase safety awareness. The aim is to enhance safety by alerting of emergency conditions. The messaging has strict latency constraints, of the order of few milliseconds, with very high reliability requirements.

In contrast, applications such as traffic and congestion monitoring require collecting information from vehicles that span multiple kilometers. The latency requirements for data delivery are relatively relaxed, *i.e.* they are "delay-tolerant", however, the physical scope of data exchange is much larger. Finally, general purpose Internet access requires connectivity to the backbone network via infrastructure such as road-side access points. These are illustrated in Figure 4.1, [64].

Recent advances in the area of Intelligent Transportation Systems (ITS) have developed the novel Dedicated Short Range Communication (DSRC) protocol, which is designed to support high speed, low latency Vehicle-to-Vehicle (V2V), and Vehicle-to-Infrastructure

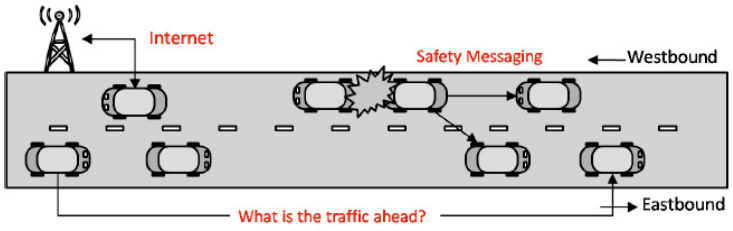


Figure 4.1: Data exchange in the VANET environment.

(V2I) communications, using the IEEE 802.11p and Wireless Access in Vehicular Environments (WAVE) standards [65].

In 1999, the Federal Communication Commission (FCC) allocated a frequency spectrum for V2BV and V2I wireless communication. DSRC is a communication service that uses the $5.850 - 5.925$ GHz band (5.9 GHz band) for the use of public safety and private applications [66].

The allocated frequency and newly developed services enable vehicles and roadside beacons to form VANETs in which the nodes can communicate wirelessly with each other without central access point.

VANETs consist of a number of vehicles traveling, and capable of communicating with each other without a fixed communication infrastructure. Therefore, VANETs are a special case of Mobile Ad-Hoc Networks (MANETs). Basically, both VANETs and MANETs are characterized by the movement and self-organization of the nodes.

However, due to driver behavior, and high speeds, VANETs characteristics are fundamentally different from typical MANETs. VANETs are characterized by rapid but somewhat predictable topology changes, with frequent fragmentation, a small effective network

diameter, and redundancy that is limited temporally and functionally.

In VANETs, there is no significant power constraint and nodes can recharge frequently. They are also characterized by highly mobile nodes, potentially large-scale network and variable network density.

VANETS are considered as one of the most prominent technologies for improving the efficiency and safety of modern transportation systems. For example, vehicles can communicate detour, traffic accident, and congestion information with nearby vehicles early to reduce traffic jam near the affected areas. VANETs applications enable vehicles to connect to the Internet to obtain real time news, traffic, and weather reports. VANETs also fuel the vast opportunities in online vehicle entertainments such as gaming and file sharing via the Internet or the local ad hoc networks.

Many factors can describe the topology of a VANET, such as the traffic density (*i.e.*, well-connected, sparsely-connected, and totally disconnected neighborhood [38]), the vehicles speed (*i.e.*, low, medium, and high speed), and the heterogeneous network environment (*i.e.*, the technologies of wireless networks around the VANET and their deployment).

In [38] Tonguz *et al.* introduce three routing parameters in order to label a vehicle driving in a VANET, on the basis of the vehicle's connectivity with other vehicles in its vicinity, for traffic scenarios in a VANET with V2V communications. No roadside infrastructure has been introduced, and vehicular communications are limited by V2V protocol. As a consequence, in totally disconnected neighborhood, vehicle communications can be provided just by V2I protocol. Roadside infrastructure is introduced by Mak *et al.* in [67], though it is limited to homogeneous network scenarios. In order to provide high bandwidth for

non-safety applications, the authors present a Medium Access Control protocol to support the multichannel operation for DSRC over IEEE 802.11 links, and no tradeoff between the use of V2V and V2I has been proposed.

In [68] a novel communication paradigm for vehicular services has been introduced. Santa *et al.* [68] consider both V2V protocol, and V2I connections; the infrastructure is limited to a basic cellular network, but no HWNs have been considered. Though V2V and V2I can be adopted in the same vehicular environment, the two protocols are not designed to cooperate for aiming vehicular communications. Similarly, Hung *et al.* in [69] introduce a HWNs infrastructure, by integrating a Wireless Metropolitan Area Network (WMAN) with VANET technology, but again, no cooperation between V2V and V2I has been proposed. In contrast, our focus is based on integration between V2V and V2I, as previously depicted by Miller in [70], though in [70] it is strongly limited by a centralized network topology of the infrastructure, where just a single vehicle is able to communicate with a RSU.

4.3 IEEE 802.11 p standard

The allocation of 75 MHz in the 5.9 GHz band for licensed DSRC in US may enable future delivery of rich media content to vehicles at short to medium ranges via V2I links [71].

Figure 4.2 shows the 75 MHz spectrum allocation in the 5.9 GHz band by the FCC in 1999 for DSRC. There are provisions for three types of channels, *i.e.* V2V channel (ch172), control channel (ch178), and V2I service channel (ch174, 176, 180, 182).

An IEEE working group is investigating a new PHY amendment of the 802.11 standard

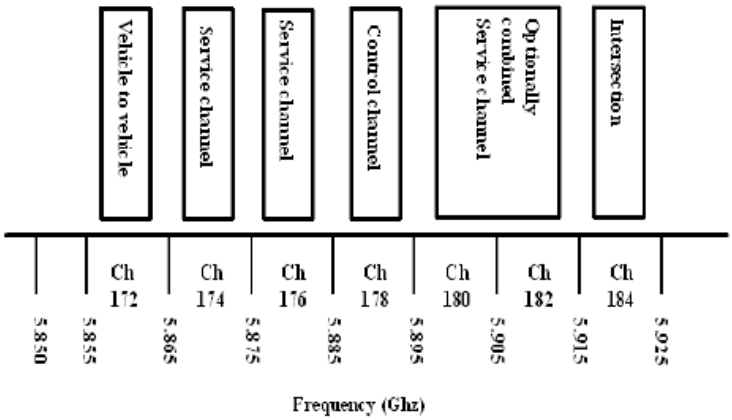


Figure 4.2: 5.9 GHz DSRC band plan with 10 MHz channels.

designed for VANETs: the Wireless Access in Vehicular Environments (WAVE), which is referred to as IEEE 802.11p [72], and [73].

Requirements for this amendment are mostly coming from vehicular Active Safety concepts and applications (communications among vehicles or between vehicles and road infrastructures), where reliability and low latency are extremely important. IEEE 802.11p should work in the $5.850 - 5.925$ GHz spectrum in North America, which is a licensed ITS Radio Services Band in the US.

By using the OFDM modulation, it provides both V2V and V2I wireless communications over distances up to 1000 m in scenarios with high velocities (up to 200 km/h), fast multipath fading and different scenarios (*i.e.* rural, highway, and city).

Operating in 10 MHz channels, it should allow data payload communication capabilities of 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbit/s, while using the optional 20 MHz channels, it achieves data payload capabilities up to 54 Mbit/s.

It is possible to directly use WLAN MAC standards for VANETs. However, the outcome

might not be satisfactory since, these mechanisms are designed without having mobility in mind. The network topology changes frequently and very fast.

Several protocols have been proposed that inherit certain parts of the existing standards but try to solve some aforementioned aspects by adding new features. IEEE 802.11 MAC [71] is based on CSMA/CA and the interframe spacing system.

The protocol is optimized by adjusting the CW dynamically to meet predefined requirements, such as maximum saturation throughput, weighted fairness, bounded delay, and differentiated QoS. The 802.11 MAC standards can overcome the hidden terminal problem in VANETs. But unfortunately, while waiting for the new IEEE 802.11p version, throughput decreases quickly in loaded and/or large networks. And because of the CSMA/CA mechanism, 802.11 cannot guarantee a deterministic upper bound on the channel access delay, which makes 802.11 not suitable for real-time traffic. Ad Hoc MAC is based on a slotted frame structure that allows for a reliable one-hop broadcast service. It easily avoids the hidden terminal problem and guarantees a relatively good QoS, which is important for real-time traffic.

It works independently from the physical layer, and can be used over the 802.11 physical layer by providing a frame structure. Relative to the IEEE 802.11 standard, the main disadvantage of ADHOC MAC is that the medium is not used efficiently, and the number of vehicles in the same communication coverage must not be greater than the number of the time slots in the frame time.

IEEE 802.11 will handle high mobility better and does not need time synchronization, while ADHOC MAC should allow higher reliability, QoS, and real-time compatibility. So,

a combination of the IEEE 802.11 standard and ADHOC MAC can provide a good and more complete solution for VANETs.

Directional-antenna-based MAC mechanisms can improve the network throughput by decreasing the transmission collisions and increasing the medium reuse possibilities. But inexpensive implementations of practical directional antenna systems are missing, which consequently makes it difficult to test and validate real directional communications over VANETs and prove these potential benefits.

4.4 Delay Tolerant Networks

A key observation in the VANET environment is the time-varying traffic density of vehicles on the roadway. The traffic density of vehicles on the roadway varies in time (day and night), and space (urban and rural area). Urban areas tend to be densely populated while rural areas have sparse traffic. Thus, connectivity in the network varies between extremes of fully connected network and a sparse network with several partitions. Furthermore, it has been shown by empirical observation, vehicles tend to travel in blocks that are separated from each other (*i.e.*, in networking terms, the nodes are partitioned from each other). As a result, message propagation in the network is constrained by the occurrence of partitions between nodes. A partitioned vehicular network is illustrated in Figure 4.3(a) [64].

Time-varying connectivity in VANETs is exploited in order to opportunistically bridge the partitions in the network, and thus to connect vehicles. When vehicles traveling in one direction are partitioned, vehicles that are traveling in the opposing direction are used to bridge, as illustrated in Figure 4.3(b).

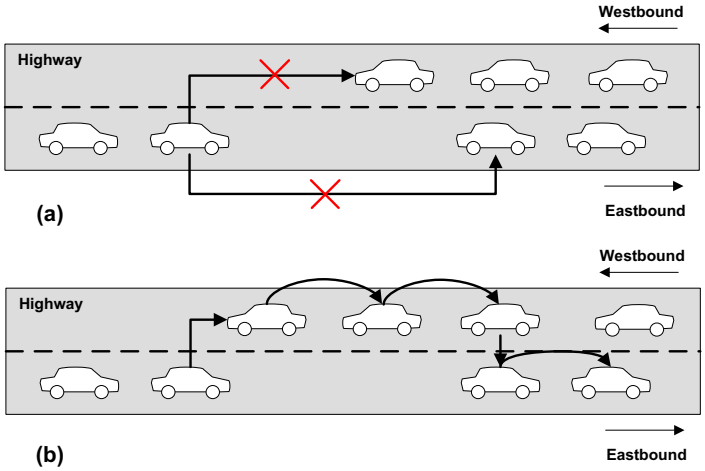


Figure 4.3: Delay tolerant network (DTN) messaging in VANET scenario. (a) Network is partitioned, and vehicles are unable to communicate. (b) Topology changes, and connectivity is finally achieved.

This transient connectivity can be used irrespective of the direction of data transfer, eastbound or westbound. However, it is important to note that this connectivity is not always instantaneously available. Partitions exist on either side of the roadway and in a sparse network there are large gaps between connected subnets.

The application of Delay Tolerant Networking (DTN) is employed in VANETs, specially for store-carry-forward mechanism and custody transfer mechanism that enable directed dissemination of data [74], [75].

The scope and requirements of applications vary significantly, and existing techniques do not essentially apply. Ongoing efforts are aimed at standardization of protocols and techniques to implement V2V, and V2I communications.

Network connectivity to *on-board* computers can be also provided via preexisting cellular and Wi-Fi cells, due to new emerging technologies, Heterogeneous Wireless Net-

work (HWN) scenarios, and multi-mode devices with several network interface cards (*e.g.*, iPhones, smartphones, Personal Digital Assistant (PDA), etc.) [76]. For this purpose, Intelligent Vehicular Ad-Hoc Networking (InVANET) defines a smart novel way of using vehicular networking by integrating on multiple wireless technologies, such as 3G cellular systems, IEEE 802.11, and IEEE 802.16e, for effective V2I communications [76].

Challenges in enabling inter-vehicle communications include high mobility rates of vehicles, large topology of the network and time-varying connectivity. There are several models discussed in related work for interconnecting vehicles on the roadway.

Dedicated Short-Range Communication (DSRC) multi-hop mode is used for V2V communications, and exploits the flooding of information of vehicular data applications [66]. Though V2V (DSRC) is envisioned by many investigators as the "traditional" protocol for VANET, connectivity disruptions can occur when vehicles are in sparse (*i.e.*, low density) and totally disconnected scenarios.

An infrastructure-based model utilizes existing or new infrastructure such as cell towers or access points (Wi-Fi) to enable messaging. Therefore V2I can represent a viable solution for some applications to bridge the inherent network fragmentation that exists in any multi-hop network formed over moving vehicles, through expensive connectivity infrastructure.

More in general, Drive-thru Internet systems represent those emerging wireless technologies providing Internet connectivity to vehicles, by temporarily connections to an access point when a vehicle cross a wireless network [77].

V2V and V2I communication technology has been developed as part of the Vehicle Infrastructure Integration (VII) initiative [78]. The VII project considers the network in-

frastructure as composed by several Road Side Unit (RSU) systems, each of them equipped with a 5.9 GHz DSRC transceiver (for communications between vehicles and RSUs), and a GPRS interface (to forward messages to the backbone networks) [78].

Due to different traffic scenarios (*i.e.* dense, sparse or totally disconnected traffic neighborhoods [38]), vehicles in VANETs move in clusters and form interconnected blocks of vehicles, [79]. As a consequence, vehicular connectivity is not always available, and messages can be lost or never received.

Opportunistic forwarding can be applied in VANETs in order to achieve connectivity between vehicles, and to forward information [62], [66], and [79]. Message propagation occurs through links built dynamically, where any vehicle can be used as next hop, and provided to forward the message to the final destination. V2V communications exploit connectivity from other neighboring vehicles, by a bridging technique [62].

Many authors have addressed the analysis of message propagation in VANETs. There are some existing routing protocols that have been explored for applications in this domain but they only focus on traditional characteristics in vehicular networks, such as mobility, traffic density, vehicle direction, and location information. This scenario represents traditional vehicular communications via V2V [62].

In [80] Resta *et al.* deals with multi-hop emergency message dissemination through a probabilistic approach. The authors derive lower bounds on the probability that a vehicle correctly receives a message within a fixed time interval. Similarly, Jiang *et al.* [81] introduce an efficient alarm message broadcast routing protocol, and estimates the receipt probability of alarm messages that are sent to vehicles.

Other works [82], and [83] analyze the message propagation model on the basis of the main VANET characteristics, such as number of hops, vehicle position, mobility, etc. Yousefi *et al.* [82] consider a single-hop dissemination protocol, based on Quality-of-Service metrics. In [83] a robust message dissemination technique is based on the position of the vehicles. Finally, Nadeem *et al.* [84] present a model of data dissemination based on bidirectional mobility on defined paths between a couple for vehicles.

In all previous works data traffic is disseminated through only vehicles communicating via V2V. No network infrastructure and V2I protocol have been considered. The use of a vehicular grid together with an infrastructure has been discussed in [85], and [86], where benefits of using the opportunistic infrastructure displaced on the roads are analyzed. Our approach relays on the network scenario depicted by Marfia *et al.* in [85], but we propose a novel protocol that provides switching from V2V to V2I, and vice versa. We expect that the message propagation via V2X be improved by a correct use of vehicular communication protocols (*i.e.*, V2V and V2I).

4.5 Vehicular-to-X Protocol

In this vision, a novel hybrid communication protocol takes place in order to maintain connectivity between vehicles moving in a VANET [7]. The proposed technique is named as Vehicular-to-X (V2X), which is based on both V2V and V2I in a vehicular networking environment.

The goals are to exploit multi-hop communications when available (via V2V), and also employ communications with network infrastructure (via V2I). A vehicle should be con-

nected via V2V or V2I on the basis of instantaneous protocol decision process, which considers traditional vehicular network attributes (*i.e.* traffic density, and message direction), and also network connectivity (*i.e.*, deployment of neighboring wireless access points, and resource utilization).

We refer to a network scenario with traditional delay tolerant networking between vehicles traveling on a highway, and a network infrastructure with overlapping heterogeneous wireless cells (*i.e.* UMTS, WiMAX, Wi-Fi, GPRS, etc.) for vehicular communication support, in order to avoid a lack of instantaneous connectivity between vehicles. On the basis of a protocol switching decision metric, the proposed protocol allows vehicles to communicate in two different ways, such as V2V, and V2I. For this purpose, we introduce an optimal path selection technique that matches the more appropriate communication protocol for a link between a vehicle and a RSU.

The proposed V2X technique deals with a hybrid protocol to aim both between vehicles (*i.e.*, V2V), and from vehicles to the infrastructure (*i.e.*, V2I) communications. The cooperation and coexistence of these two different methods can assure a good connectivity in VANET scenarios. As a matter, in sparsely-connected and totally-disconnected neighborhoods, V2V communications are not always available [66], and the V2I represents a solution in order to avoid dropped connections.

In our goal, we extend the three traditional traffic density scenarios, as depicted in [38], with a HWN infrastructure with overlapping wireless cells. No fixed displacement of access points in the ground has been considered, as assumed in [87]; we want to represent a real outdoor and urban network scenario, where wireless networks are overlapping, and partially

or totally covering the VANET (see Figure 4.4).

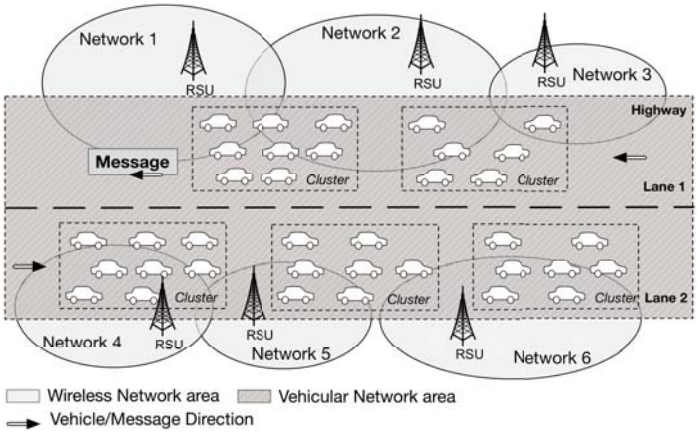


Figure 4.4: Heterogenous wireless network scenario, with different network technologies and overlapping wireless cells.

Three main communication models characterize a VANET [88]. In this paper, we deal with the hybrid model in which several RSUs of different wireless technologies are deployed in order to partially cover a given area. In the proposed V2X protocol, each vehicle can communicate via V2V or V2I, on the basis of a decision taken by the vehicle itself.

The V2X protocol exploits both the V2V and the V2I connectivity, and the switching from one to the other is performed on the basis of a switching decision metric. The local information comprises the key data defining the network scenario. The local information describes the traffic density as directly experienced by the vehicle, and can be established by periodic "hello" messages, sent in the vehicular network [38].

Each vehicle continuously monitors its local connectivity by storing the received broadcast messages. Assuming local information as global provides knowledge about topology and traffic of the network scenario. Obviously, the network scenario is updated on the basis

of vehicle's mobility pattern. By assuming a preexistent network infrastructure, we define a routing parameter, called as *Infrastructure Connectivity* (IC), which gives information about the actual vehicle ability to be directly connected with an RSU.

If a vehicle has IC = 1, then the vehicle is inside the radio coverage of a wireless cell and it is potentially able to directly connect to the RSU associated with the neighboring wireless cell. It does not mean that the vehicle is connected with the RSU, but just that it is under wireless cell coverage. Moreover, if a vehicle is in the range of more than one RSU, then the value of IC will be always 1. So, IC is not representative of how many wireless cells are near the vehicle, but just that there are available neighboring wireless cells. If IC = 1, then the vehicle can enhance its connectivity in order to:

(*a*) Store messages to the RSU,(*i.e.*, specially for sparsely or totally disconnected scenarios);

(*b*) Receive messages from the RSU, (*i.e.*, specially for sparsely or totally disconnected scenarios);

(*c*) Work as a "bridge" to connect other vehicles moving in the same cluster directly to the RSUs (*i.e.*, specially for locally dense traffic scenarios).

Finally, the value of IC is set to 0 when no wireless cell is near the vehicle.

4.5.1 Protocol Switching Decision metric

After describing the network scenario, in this subsection we deal with a protocol switching decision metric, which evaluates if and when to employ the V2V and the V2I protocols.

As V2X is based on both V2V and V2I, we assume that a vehicle is in a state s when is connected via V2V, or V2I protocol, respectively.

Let S be a set of two states $S = \{\mathbf{s}_{\mathrm{V2V}}, \mathbf{s}_{\mathrm{V2I}}\}$, where:

- $\mathbf{s}_{\mathrm{V2V}}$ represents the state "connected via V2V", that means a vehicle is connected to the vehicular network and served by V2V protocol. This state does not carry on any information about neither the actual density traffic scenario or the presence of candidate neighboring wireless networks;

- $\mathbf{s}_{\mathrm{V2I}}$ represents the state "connected via V2I", that means a vehicle is connected to a neighboring wireless network and served by V2I protocol. This state does not give any information about the actual density traffic scenario. The protocol switching from a serving protocol to a new one (*i.e.* from V2V to V2I, or vice versa) is expressed by an action a, which represents a state switching.

Figure 4.5 shows the relationships among states and actions.

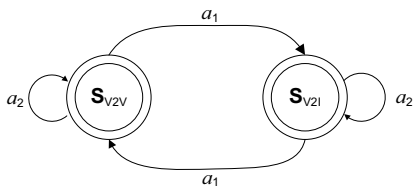


Figure 4.5: Relationship among states and actions, for protocol switching decisions in V2X.

Let us consider A as a set of two actions $S = \{a_1, a_2\}$, where:

- a_1 represents the decision *Make-a-Protocol-Switching* (*i.e.* called as MPS) taken by

the vehicle to switch from V2V to V2I, and vice versa;

- a_2 represents the decision *Maintain-the-Serving-Protocol* (*i.e.* called as MSP) taken by the vehicle. It means that the vehicle does not change the serving protocol.

Several factors can affect the choice of an action a, such as (*i*) the value of the Infrastructure Connectivity parameter, (*ii*) the candidate neighboring wireless networks, and (*iii*) the traffic density, such as:

(*i*) If a vehicle is served by V2V and has the IC = 1, then a protocol switching decision can be taken in order to switch to V2I (*i.e.*, by MPS action). Otherwise, if IC = 0, no wireless cell is available near the vehicle, and then it will be just served by the V2V if still available (*i.e.*, by MSP action);

(*ii*) If a vehicle has IC = 1, then one or more neighboring wireless networks are available. The vehicle should choose the more appropriate network according to its requirements, and then perform an MPS action;

(*iii*) If a vehicle is in a dense or sparse traffic neighborhood and has IC = 1, it could decide for both the two actions, (*i.e.* MPS, and MSP). While if a vehicle is in a totally disconnected neighborhood and has IC = 1, it should decide for a MPS and be connected to V2I.

As we can notice, the protocol switching decision is a big deal to take into account.

In order to consider and obtain the more appropriate protocol switching decision, in the following Subsection 4.5.2 we are defining our optimal path selection technique.

4.5.2 Optimal path selection technique

Our *optimal path selection technique* represents a policy in order to decide for the optimal vehicular communication protocol between two end nodes. In [89] Kherani *et al.* present an optimal path criterion, but no channel measurements have been considered. In contrast, the proposed optimal path selection technique is based on a total cost function, that is a linear combination of two physical parameters, such as (i) the radio resource utilization time, and (ii) the time interval needed to transmit a message over a path. An optimal path connecting the i-th vehicle to the k-th RSU via multi-hop is selected on the basis of a minimization process of the total cost function.

This technique gives information about how a vehicle can be connected to a particular RSU, which is placed along the same moving direction of the vehicle; moreover, this criterion does not depend on the particular technology of the wireless cell. Figure 4.6 depicts our case study. Vehicle A is the source of message propagation to the RSU of a wireless cell. The vehicle A with IC = 0 can communicate with its next one-hop neighbors via V2V, in order to reach the RSU.

Two paths to RSU are drawn: the first one is from vehicle A to B, C, and finally RSU; the second one is from vehicle A to D, E, F, G, and then RSU.

For the connectivity link from the i-th to the j-th vehicle we define as *link utilization time* $\delta_{(i,j)}$ the time needed to transmit a message of length L [bit] from the i-th to the j-th vehicle, such as

$$\delta_{(i,j)} = \frac{L}{f_{(i,j)}}, \tag{4.1}$$

where $f_{(i,j)}$ is the actual data rate for a particular link [Mbit/s]. We note that, for a link

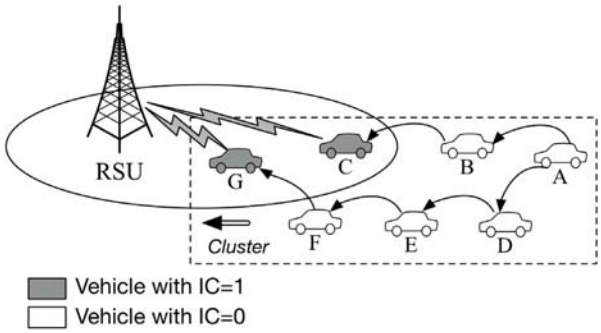


Figure 4.6: Multi-hop scenario.

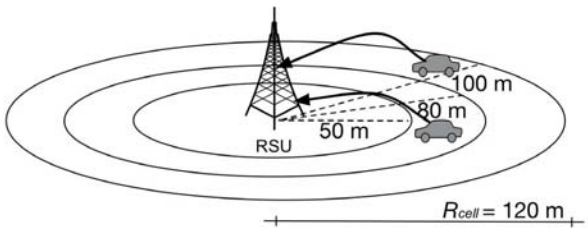


Figure 4.7: Data Rate Reduction depends on the distance from a vehicle to the RSU.

Table 4.1: Data Rate Reduction factor versus the path length

Wireless Network	R_{cell}	Distance vehicle-RSU	Data Rate Reduction
Wi-Fi	120 m	$[0, 50)$ m	10%
		$[50, 80)$ m	15%
		$[80, 100)$ m	30%
UMTS	600 m	$[0, 300)$ m	20%
		$[300, 400)$ m	25%
		$[400, 600)$ m	35%

between a vehicle and an RSU, $f_{(i,j)}$ can be obtained by the nominal data rate $\breve{f}_{(i,j)}$ by applying a *Data Rate Reduction* factor (*i.e.* $\rho_{(i,j)}$) that depends on the distance from the vehicle to the RSU, namely:

$$f_{(i,j)} = \rho_{(i,j)} \breve{f}_{(i,j)}. \tag{4.2}$$

Table 4.1 collects our assumptions for the Data Rate Reduction factor, where R_{cell} is the wireless cell range corresponding to the nominal data rate $\breve{f}_{(i,j)}$ for a given access technology. The Data Rate Reduction factor increases when a vehicle is laying in the bound of a wireless cell.

Let us consider a cluster C composed by a set S of vehicles (*i.e.*, $S = 1, 2, \ldots, n$). Moreover, m RSUs (*i.e.*, $m < n$) are displaced in the network scenario as depicted in Figure 4.4. Each vehicle is assumed to be able to communicate with all the other vehicles around it via V2V, on the basis of a connectivity bond expressed in [88]. We also assume that not all the vehicles in the cluster are able to connect to an RSU via V2I (*e.g.* not all the vehicles have an appropriate network interface card and/or are in the range of an RSU), but only a subset of them $S' = \{1, 2, \ldots, l\} \subset S$, with $l < n$.

Let $\mathbf{N}_{[n \times n]}$ be the matrix of the V2V transmitting data rates between vehicles in the cluster C (*i.e.*, for $f_{(i,j)} \neq 0$, for $i \neq j$, and for $f_{(i,j)} = 0$ for $i = j$, with $i, j = \{1, 2, \ldots, n\}$),

$$\mathbf{N}_{[n \times n]} = \begin{bmatrix} 0 & f_{(1,2)} & \ldots & f_{(1,n)} \\ f_{(2,1)} & 0 & \ldots & f_{(2,n)} \\ \ldots & \ldots & 0 & \ldots \\ f_{(n,1)} & f_{(n,2)} & \ldots & 0 \end{bmatrix}. \tag{4.3}$$

Moreover, let $\mathbf{M}_{[n\times m]}$ be the matrix of V2I transmitting data rates,

$$\mathbf{M}_{[n\times m]} = \begin{bmatrix} \tilde{f}_{(1,1)} & \cdots & \tilde{f}_{(1,m)} \\ \tilde{f}_{(2,1)} & \cdots & \tilde{f}_{(2,m)} \\ \cdots & \cdots & \cdots \\ \tilde{f}_{(n,1)} & \cdots & \tilde{f}_{(n,m)} \end{bmatrix}, \tag{4.4}$$

where $\tilde{f}_{(i,k)}$ is the data rate associated to the link from the i-th vehicle to the k-th RSU (*e.g.* links from grey vehicles to the RSU in Figure 4.6).

Elements $\tilde{f}_{(i,k)}$ in matrix $\mathbf{M}$ will be null when there is no connection between i-th vehicle to k-th RSU. According to typical cellular systems like UMTS, a vehicle can be simultaneously connected to more than one single RSU. So, we assume the index k for the RSUs as $k = \{1, 2, \ldots, h\}$ with $h < m$. Then, as l vehicles have IC=1, for $i = \{1, 2, \ldots, l\}$, and $k = \{1, 2, \ldots, h\}$, will be not null.

From (4.3) and (4.4), we can define the matrix $\mathbf{D}_{[n\times m]}$ of transmitting data rates for the i-th vehicle in the cluster C, as follows:

$$\mathbf{D}_{[n\times m]} = \left[\mathbf{N}_{[n\times n]} \middle| \mathbf{M}_{[n\times m]}\right] = \left[\begin{array}{cccc|ccc} 0 & f_{(1,2)} & \cdots & f_{(1,n)} & \tilde{f}_{(1,1)} & \cdots & \tilde{f}_{(1,m)} \\ f_{(2,1)} & 0 & \cdots & f_{(2,n)} & \tilde{f}_{(2,1)} & \cdots & \tilde{f}_{(2,m)} \\ \cdots & \cdots & 0 & \cdots & \cdots & \cdots & \cdots \\ f_{(n,1)} & f_{(n,2)} & \cdots & 0 & \tilde{f}_{(n,1)} & \cdots & \tilde{f}_{(n,m)} \end{array}\right], \tag{4.5}$$

where each element represents the direct link from the i-th vehicle to the j-th vehicle, or to the k-th RSU (*i.e.*,$f_{(i,j)}$, or $\tilde{f}_{(i,k)}$, respectively). As a consequence, a path from the i-th vehicle to the k-th RSU will exist if for each hop that composes the path the transmitting data rate is non-null. We also evince that the maximum number of directed links from a

vehicle to an RSU is $d = l \cdot h$, while the maximum number of different paths that can connect the i-th vehicle to the k-th RSU is $n \cdot d$.

Now, let us denote with $\Gamma_{i,j}^{(k)}$ the k-path from the i-th to the j-th node, either vehicle or RSU, consisting in the sequence of M nodes $\left[u_1^{(k)}, u_2^{(k)}, \ldots, u_t^{(k)}, u_{t+1}^{(k)}, \ldots, u_M^{(k)}\right]$, with $u_1^{(k)} = i$, and $u_M^{(k)} = j$.

The path length for $\Gamma_{i,j}^{(k)}$ represents the number of hops M for a single path.

Let us assume a first partition of $\Gamma_{i,j}^{(k)}$ into Φ_k sets $\gamma_\varphi^{(k)}$, with $\varphi = \{1, 2, \ldots, \Phi_k\}$; each set consists of those $\mu_\varphi^{(k)}$ links sharing the same frequency band F_φ [Hz], namely,

$$\gamma_\varphi^{(k)} = \left\{ \left(u_{\varphi_1}, u_{\varphi_2}\right), \ldots, \left(u_{\varphi_{\mu_h^{(k)}-1}}, u_{\varphi_{\mu_h^{(k)}}}\right) \right\}, \quad \varphi = 1, 2, \ldots, \Phi_k \tag{4.6}$$

We note that each subset $\gamma_\varphi^{(k)}$ is homogeneous with respect to the wireless technology and standard, (*e.g.*, IEEE 802.11p, GSM-GPRS, UMTS, HSDPA, UMTS LTE, WiMAX, etc.).

Then, for each set $\gamma_\varphi^{(k)}$, let $\nu_\varphi^{(k)}$ be the number of subsets $\eta_S^{(k,\varphi)}$ (*i.e.*, $s = \left\{1, 2, \ldots, \nu_\varphi^{(k)}\right\}$), such as

$$\eta_s^{(k,\varphi)} = \left\{ q_{s,1}^{(k,\varphi)}, q_{s,2}^{(k,\varphi)}, \ldots, q_{s,Z_s^{(k,\varphi)}}^{(k,\varphi)} \right\}, \tag{4.7}$$

where the s-th subset $\eta_S^{(k,\varphi)}$ consists of those $q_{s,\xi}^{(k,\varphi)}$ links

$$q_{s,\xi}^{(k,\varphi)} = \left(u_{\zeta_{s,\xi}^{(k,\varphi)}}, u_{\tau_{s,\xi}^{(k,\varphi)}}\right), \quad \xi = 1, 2, \ldots, Z_s^{(k,\varphi)} \tag{4.8}$$

for which simultaneous use of the wireless channel is not possible. This is for instance the case of IEEE 802.11 links connecting a given node to its 1-hop neighbors.

Analogously to (4.1), for each set $\gamma_\varphi^{(k)}$ we define as *radio resource utilization time* (*i.e.*, $Q_\varphi^{(k)}$ [s]) for a message of length equal to L [bit] the quantity:

$$Q_{\varphi}^{(k)} = \underset{1 \le s \le \nu_{\varphi}^{(k)}}{Max} \left[\sum_{q_{s,\xi}^{(k,\varphi)} \in \eta_s^{(k,\varphi)}} \frac{L}{f_{\left(q_{s,\xi}^{(k,\varphi)}\right)}} \right], \tag{4.9}$$

where $f_{\left(q_{s,\xi}^{(k,\varphi)}\right)}$ represents the data rate for each link $q_{s,\xi}^{(k,\varphi)}$.

As it follows, for each path $\Gamma_{i,j}^{(k)}$ we define as weighted total utilization time (*i.e.* $\tilde{Q}_{i,j}^{(k)}$, [s]) the sum of each weighted *radio resource utilization time* that composes the path, such as

$$\tilde{Q}_{i,j}^{(k)} = \sum_{\varphi=1}^{\Phi_k} C_{\varphi} \cdot Q_{\varphi}^{(k)}, \tag{4.10}$$

where C_{φ} is the relative cost associated to the φ-th frequency band. In general, the cost will be proportional to the allocated bandwidth; moreover, it may also depend on the access network technology (*e.g.*, Wi-Fi, and UMTS).

In addition, let us denote with $D_{i,j}^{(k)}$ the time needed to transmit over $\gamma_{i,j}^{(k)}$ a message of length equal to L [bit]. Apart from latencies introduced by node processing and queuing, the following relation represents the *delay factor* $D_{i,j}^{(k)}$ on a single link (i, j),

$$D_{i,j}^{(k)} = \sum_{\varphi=1}^{\Phi_k} \sum_{s=1}^{\mu_{\varphi}^{(k)}-1} \frac{L}{f_{\left(u_{\varphi s}, u_{\varphi s+1}\right)}}. \tag{4.11}$$

Finally, we define $\Lambda_{i,j}^{(k)}$ [s] the *total cost function* associated to the path $\gamma_{i,j}^{(k)}$, as the linear combination of the *weighted total utilization time* $\tilde{Q}_{i,j}^{(k)}$ [s], and the delay $D_{i,j}^{(k)}$ [s], such as

$$\Lambda_{i,j}^{(k)} = \alpha \tilde{Q}_{i,j}^{(k)} + (1 - \alpha) D_{i,j}^{(k)}, \tag{4.12}$$

where $0 \le \alpha \le 1$ is a weight given to $\tilde{Q}_{i,j}^{(k)}$ with respect to the *delay factor*. Thus, for a given pair of nodes (i, j), the selected path will be the one, among all the nd paths, minimizing the *total cost function*. For different values of α (*i.e.*, $\alpha = [0, 0.5, 1]$), (4.12) becomes,

$$\Lambda_{i,j}^{(k)} = \begin{cases} D_{i,j}^{(k)}, & \alpha = 0 \\ \alpha \tilde{Q}_{i,j}^{(k)} + (1-\alpha)\, D_{i,j}^{(k)}, & 0 < \alpha < 1 \\ \tilde{Q}_{i,j}^{(k)}, & \alpha = 1 \end{cases} \tag{4.13}$$

We will show simulation results evaluated for $\alpha = 0$.

4.5.3 Simulation Results

In this Subsection we show results about our V2X protocol. Particularly we evaluate the *total cost function* for the optimum path selection in two different network scenarios, such as (i) a *dense*, and (ii) *sparse* traffic one.

In both cases, we have considered a set S of vehicles (*i.e.*, $S = \{s_1, s_{2,} \ldots, s_{10}\}$), and one RSU (*i.e.*, an UMTS base station). We have also assumed S' as a subset of vehicles with a direct connection with an RSU, whose transmission rates have been chosen equal to 1 kbits/s.

From (4.5) the matrix $\mathbf{D}_{[n\times m]}$ (*i.e.*, with $n = 10$, and $m = 1$) has symmetric elements given by $\mathbf{D}_{[n\times n]}$, (*i.e.*, $f_{(i,j)} = f_{(j,i)}$ in the transmission range $[2.0, 4.25]$ kbits/s), while the matrix $\mathbf{M}_{[n\times m]}$ is a single column with some null elements.

In the following, we list the main parameters employed in the simulations:

- In *dense* traffic scenario, $f_{(i,j)}$ are non-null, with $i \neq j$;
- In *sparse* traffic scenario, few elements $f_{(i,j)}$ are null, for $i \neq j$, depending on the number of vehicles connected with other vehicles. Through this information is unknown *a priori*, we have assumed that a vehicle can learn about its neighboring vehicles.

Table 4.2 collects the connection links that we have assumed, for each vehicle in sparse traffic scenario (*i.e.* the value 1 means there is an available link, otherwise no connection is available).

As defined in Subsection 4.5.1, the parameter IC is set equal to 1 when a vehicle is inside a wireless cell range, while a vehicle with IC = 0 is connected via V2V if the radio range is under 125 m [88].

Figure 4.8 depicts an example of connectivity for vehicles with IC = 0 (white vehicles), and IC = 1 (grey vehicles) in a *sparse* traffic scenario. Vehicle #1 is connected only with some vehicles, which are in its range of visibility (*i.e.*, it means that the distance between vehicle #1 and #5 is less than 125 m).

We have assumed that all the j-th even vehicles (*i.e.*, $j = 2, 4, 6, 8$, and 10) have IC = 1, while the l-th odd vehicles (*i.e.*, $l = 1, 3, 5, 7$ and 9) have IC = 0. As a consequence, the even vehicles represent a necessary hop for all the vehicles with IC = 0, in order to reach the RSU, and send a message whose length is L (*i.e.*, $L = 300$ [bit]).

By assuming five vehicles with IC = 0, and other five vehicles with IC = 1, the simulated scenario has 50% of the vehicles potentially connected via V2I. The other 50% of vehicles is totally/partially connected with other vehicles via V2V (in *dense*/*sparse* traffic scenario, respectively).

In the simulation results, the maximum number of different paths for each vehicle is 5 (*i.e.*, nd paths). The vehicles with IC = 1 can reach the RSU (i) through a direct link (*i.e.* by using V2I), or (ii) via multi-hop for at least one hop (*i.e.* by using V2V). The vehicles with IC = 0 can be connected to the RSU only through multi-hop (*i.e.*, by using

Table 4.2: Connectivity links in a *sparse* traffic scenario.

Vehicle ID	1	2	3	4	5	6	7	8	9	10
1			1	1	1		1	1	1	1
2				1	1	1		1	1	1
3	1				1	1	1		1	1
4	1	1				1	1	1		1
5	1	1	1				1	1	1	
6		1	1	1				1	1	1
7	1		1	1	1				1	1
8	1	1		1	1	1				1
9	1	1	1		1	1	1			
10	1	1	1	1		1	1	1		

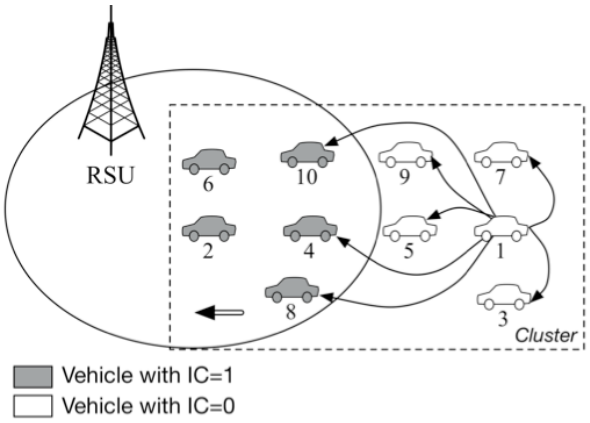


Figure 4.8: Example of V2V and V2I connectivity in a *sparse* traffic scenario.

V2V). Finally, the optimal path will be that one minimizing the (*total cost function* $\Lambda_{i,j}^{(k)}$, as expressed in (4.12).

Table 4.3 collects the values of the total cost function in a *dense* traffic scenario, for all the available paths originated from vehicles with IC = 1 (*i.e.*, vehicle #2, #4, #6, #8 and #10). As expressed in (4.13), for $\alpha = 0$ the total cost function corresponds to the delay factor, *i.e.* $\Lambda_{i,j}^{(k)} = D_{i,j}^{(k)}$.

The maximum value of the delay factor is 0.3 s, which is obtained when one of such vehicles is connected via V2I; as an example, for vehicle #2 the path 1 corresponds to a direct link to the RSU, and the delay factor is

$$D_{2,\text{RSU}}^{(1)} = \frac{L}{f_{(2,\text{RSU})}} = \frac{300}{1000} = 0.3 \quad [\text{s}]. \tag{4.14}$$

On the contrary, low values of the delay are obtained when a vehicle is connected via V2V, and reaches the RSU through at least one hop (*e.g.*, path 2, 3, 4, and 5 from vehicle #2 to the RSU).

In Table 4.4, we list the values of the total cost function in a dense traffic scenario, for vehicles with IC = 0. It has low values in the range $[0.046, 0.125]$ seconds. In this case, each vehicle is being connecting to the RSU via V2V through at least one hop.

By a comparison between Table 4.3 and 4.4, we evince that in *dense* traffic scenario low values of the total cost function are obtained for V2V protocol, while the maximum value is for V2I protocol.

Figure 4.9(a) and 4.9(b) depict some values of the total cost function for vehicles with IC = 1 (*i.e.*, vehicle #2), and IC = 0 (*i.e.*, vehicle #1), respectively. Vehicles connected to the RSU via V2V follows paths with low delays, while for vehicles connected directly to

Vehicle ID	path 1	path 2	path 3	path 4	path 5
#2	0.3	0.066	0.066	0.066	0.085
#4	0.066	0.3	0.046	0.046	0.075
#6	0.06	0.046	0.3	0.046	0.046
#8	0.06	0.046	0.046	0.3	0.046
#10	0.085	0.075	0.046	0.046	0.3

Table 4.3: Values of total cost function [s] for vehicles with IC = 1, in a *dense* traffic scenario.

Vehicle ID	path 1	path 2	path 3	path 4	path 5
#1	0.125	0.085	0.066	0.085	0.125
#3	0.085	0.066	0.046	0.066	0.066
#5	0.075	0.075	0.046	0.046	0.046
#7	0.06	0.046	0.046	0.046	0.046
#9	0.085	0.046	0.046	0.046	0.046

Table 4.4: Values of total cost function [s] for vehicles with IC=0, in a *dense* traffic scenario.

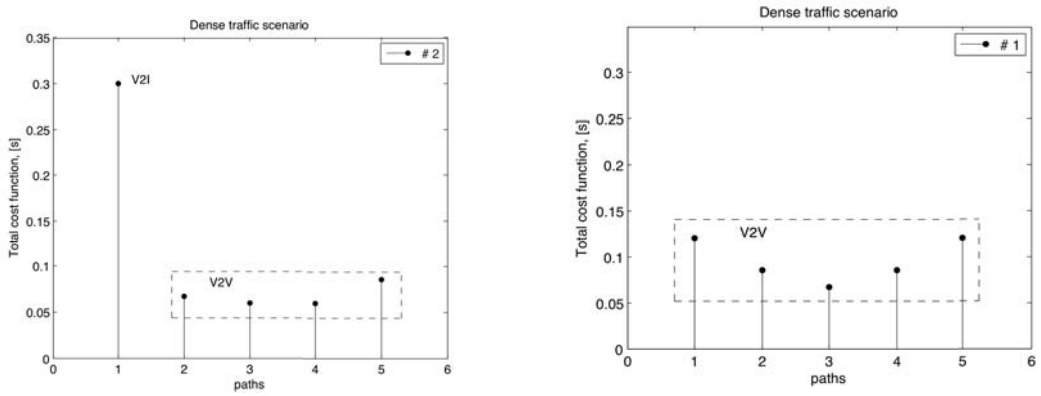
the RSU via V2I the total cost function has high value (see Figure 4.9(a)). Low values of $\Lambda_{i,j}^{(k)}$ are obtained also for vehicles with IC = 0, which are communicating to the RSU via V2V (see Figure 4.9(b)).

In Table 4.5 we have collected the values of $\Lambda_{i,j}^{(k)}$ for $\alpha = 0$, *sparse* traffic scenario and vehicles with IC = 1. The maximum value is still 0.3 s, obtained when a vehicle is connected via V2I; in contrast, low values are obtained when a vehicle is in V2V state. From this, we can conclude that also in a sparse traffic scenario with $\alpha = 0$, for vehicles with IC = 1, V2V is preferred to V2I.

A different result is obtained in a sparse traffic scenario for vehicles with IC = 0. Table 4.6 lists the values of the total cost function for different paths; in this case, the maximum value occurs for several paths when a vehicle is connected via V2V to the RSU. Table 4.2 collects the single connections for each vehicle in a sparse traffic scenario. The maximum value of the total cost function is obtained when a vehicle uses V2V in order to reach the RSU (*e.g.*, the vehicle #3 is connected via V2V to vehicles #2, #4, and #8; or the vehicle #5 is connected via multi-hop to vehicles #4, #6, and #10, etc.), with more than one single hop.

In contrast, the minimum values of the total cost function are obtained when a vehicle is directly connected to a vehicle with IC=1 (*e.g.*, the vehicle #3 is connected via V2V to vehicle #6, and #10), and so V2V is used for just one single hop.

In Figure 4.10(a) and 4.10(b), we show some values of $\Lambda_{i,j}^{(k)}$ for vehicles with IC = 1 (*i.e.*, vehicle #2), and IC=0 (*i.e.*, vehicle #1), in a *sparse* traffic scenarios, respectively. Analogously to Figure 4.9(a), V2I has high values of the *total cost function* (see Figure 4.10(a)),



(a) Vehicles with IC=1.

(b) Vehicles with IC=0.

Figure 4.9: Optimal path selection technique ($\alpha = 0$) in a *dense* traffic scenario.

Vehicle ID	path 1	path 2	path 3	path 4	path 5
#2	0.3	0.092	0.092	0.092	0.075
#4	0.092	0.3	0.1	0.1	0.066
#6	0.092	0.1	0.3	0.1	0.1
#8	0.092	0.1	0.1	0.3	0.1
#10	0.075	0.066	0.1	0.1	0.3

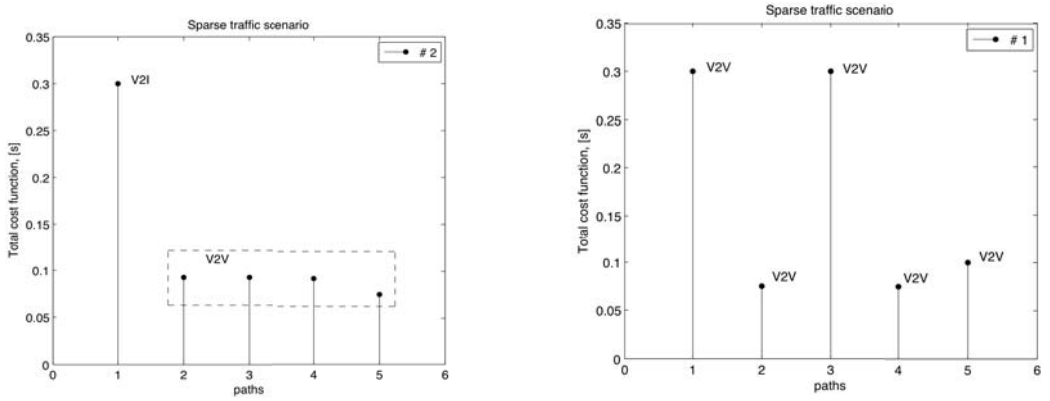
Table 4.5: Values of total cost function [s] for vehicles with IC = 1, in a *sparse* traffic scenario.

Vehicle ID	path 1	path 2	path 3	path 4	path 5
#1	0.3	0.075	0.3	0.075	0.1
#3	0.3	0.3	0.1	0.1	0.092
#5	0.066	0.3	0.3	0.1	0.3
#7	0.3	0.1	0.3	0.3	0.1
#9	0.075	0.3	0.1	0.3	0.3

Table 4.6: Values of total cost function [s] for vehicles with IC = 0, in a *sparse* traffic scenario.

while for vehicles with IC = 0, V2V has high values when the number of hops in a path is increasing (see Figure 4.10(b)).

As a conclusion, in a *sparse* traffic scenario, the optimum path can guarantee a minimum *total cost function* equal to 0.066 s for vehicles connected via V2V. In dense traffic scenario, the optimum path takes a minimum total cost function equal to 0.046 s for vehicles connected via V2V. High values of the total cost function are obtained with V2I in a dense traffic scenario, and with V2V in a sparse traffic scenario for increasing number of hops.



(a) Vehicles with IC=1.

(b) Vehicles with IC=0.

Figure 4.10: Optimal path selection technique ($\alpha = 0$) in a *sparse* traffic scenario.

4.6 Opportunistic vehicular networking

Opportunistic forwarding networking techniques can be applied in VANETs in order to achieve connectivity between vehicles [62], [79], [90], [91].

Message propagation occurs through links built dynamically, where any vehicle can opportunistically be used as next hop, and provided to forward the message to the final destination. In such scenario, V2V communications opportunistically exploit connectivity from other neighboring vehicles, by a bridging technique [62, 90].

Many authors have addressed the analysis of message propagation in VANETs. The main challenge is how the information is forwarded when the connectivity is difficult to maintain [92]. There are some existing routing protocols that have been explored for applications in this domain but they only focus on traditional characteristics in vehicular networks, such as mobility, traffic density, vehicle direction, and location information. This scenario represents traditional vehicular communications via V2V [62].

In [80] Resta *et al.* deals with multi-hop emergency message dissemination in VANETs, through a probability approach. The authors derive lower bounds on the probability that a vehicle correctly receives a message within a fixed time interval. As the same, Jiang *et al.* [81] introduces an efficient alarm message broadcast routing for VANET. This technique estimates the receipt probability of alarm messages that are sent to vehicles. Other works [82], [83], and [84] analyze the message propagation model on the basis of the main VANET characteristics, such as number of hops, vehicle's position, mobility, etc.

In [82] a dissemination protocol has been proposed, where vehicles are sending beacon messages periodically to announce to other vehicles their current situation, and using received messages to prevent possible unsafe situations. Yousefi *et al.* [82] consider a single-hop dissemination protocol, and also quality-of-service metrics, like delivery rate and delay. In [83] the authors analyze how to achieve robust message dissemination in VANET, with vehicular traffic independency, based on the position of the vehicles. Finally, Nadeem *et al.* [84] present a model of data dissemination based on bidirectional mobility on defined paths between a couple for vehicles. Therefore, in all previous works data traffic is disseminated through only vehicles moving in the VANET, which are communicating via V2V. No network infrastructure and V2I protocol have been considered.

The use of a vehicular grid together with an infrastructure has been discussed in [85, 86]. Marfia *et al.* analyze the benefits of using the opportunistic infrastructure provided by access points displaced on the roads. Our approach relays on the network scenario depicted in [85], but we consider vehicles communicating via the novel protocol V2X, and then we analyze how a message is forwarded from a source vehicle to a destination vehicle. We

expect that the message propagation via V2X be improved by a correct use of vehicular communication protocols, (*i.e.*, V2V and V2I).

4.7 Message Propagation Rates with V2X protocol

In this Section we shall analyze how an information message is forwarded by vehicles communicating via V2X protocol.

We characterize the bounds of information propagation, and compare performance with traditional message propagation based on opportunistic networking. Simulation results show the effectiveness of the proposed hybrid vehicular communication protocol V2X.

As previously discussed, we refer to Figure 4.4 which represents a typical vehicular network scenario, partially covered by the preexistent wireless network infrastructure. Different technologies are considered for typical RSUs, such as UMTS, IEEE 802.11, and WiMAX.

Particularly, in Figure 4.4 we have assumed IEEE 802.11p RSUs, whose radio coverage is around 1000 m, and are displaced at a distance of 500 m each other. As defined in [62], the highway behavior of vehicles is depicted by clusters, whose cardinality of each block is related to the vehicle density. Vehicles are traveling in two separated lanes (*i.e.*, lane 1, and 2), and we define north (*i.e.*, N), and south (*i.e.*, S) directions, as the directions long the lane 1, and 2, respectively.

Each vehicle is able to communicate via V2V or V2I, on the basis of the proposed switching protocol decision.

Let us assume the vehicles are traveling at a constant velocity c [m/s], while v is the

message propagation rate within a cluster, such as:

$$v = \frac{x}{t}, \tag{4.15}$$

where x is the transmission range distance between two consecutive and connected vehicles (*i.e.*, $0 < x < 125$ m, according to [62]), and t is the time necessary for a successful transmission [s].

Basically, as in a cluster each couple of connected vehicles is communicating in a particular link (*i.e.*, named as (i, j), from the i-th to the j-th vehicle), the time t for a successful transmission will not be the same for each couple of communicating vehicles in the same cluster. Moreover, the variable t also corresponds to the link utilization time (*i.e.*, $q_{(i,j)}$, [s]), that is the time necessary to send a message of length L [bit], over the transmitting data rate for (i, j) link, (*i.e.*, $f_{(i,j)}$ [Mbit/s]), whose expression is

$$q_{(i,j)} = \frac{L}{f_{(i,j)}}, \tag{4.16}$$

As a consequence, the message propagation rate within a cluster should consider each single contribution due to a single link (i, j). Therefore, the expression of v depends on the average message propagation rate for each hop within a cluster. Equation (4.15) becomes:

$$v = \frac{1}{h} \sum_{i,j} v_{(i,j)} = \frac{1}{h} \sum_{i,j} \frac{x_{(i,j)}}{q_{(i,j)}} = \frac{1}{hL} \sum_{i,j} x_{(i,j)} \cdot f_{(i,j)}. \tag{4.17}$$

where $v_{(i,j)}$ is the message propagation rate for the link (i, j), and h is the number of hops occurred within a cluster.

We define a path $P_{(i,l)}$, as a set of h links that connect the i-th vehicle to the l-th vehicle. Therefore, the path utilization time, $Q\left[P_{(i,l)}\right]$, is the overall necessary time to

send a message L over a path $P_{(i,l)}$, such as

$$Q\left[P_{(i,l)}\right] = \sum_{i \neq j}^{j=l} q_{(i,j)} = L \sum_{i \neq j}^{j=l} \frac{1}{f_{(i,j)}}. \tag{4.18}$$

As noticeable, the message propagation rate v inside a cluster is increasing when the number of hops h, or the path utilization time, is low; it follows that an optimal path detection technique is an important issue for opportunistic networking in VANET [89].

Now, let us define v_{RSU} as the message propagation rate within the network infrastructure, as

$$v_{\mathrm{RSU}} = \frac{d}{T} \tag{4.19}$$

where d is the distance between two consecutive RSUs (*i.e.*, $d = 500$ m), and T represents the time necessary to forward a message between two consecutive RSUs. The value of T is represented by the ratio between the length of the message L [bit], and the effective data rate (*i.e.*, B [bit/s]), for the link between the m-th and $(m+1)$-th RSU. Equation (4.19) becomes:

$$v_{\mathrm{RSU}} = \frac{d \cdot B}{L}. \tag{4.20}$$

In (4.19), the message propagation rate inside the network infrastructure is strictly dependent on the message propagation direction, and a message is forwarded to an RSU placed along the same message propagation direction.

An RSU that receives a message by a vehicle can forward it to the next RSU, displaced on the same message direction. The potentiality of communications between RSUs has been introduced in order to avoid connectivity interruptions caused by low traffic densities, and that the V2V protocol cannot always solve [66].

In general, (4.19) represents the message propagation rate within the preexistent network infrastructure. Moreover, we should also consider the message propagation rate in *uplink* (*downlink*), when a vehicle sends a message to an RSU, (and vice versa). The message propagation rates in *uplink* and *downlink* are, respectively:

$$v_{\mathrm{UP}} = \frac{x_r}{t_{\mathrm{UP}}} = \frac{x_r}{L} \cdot \tilde{f}_{(i,m)}, \qquad v_{\mathrm{DOWN}} = \frac{x_r}{t_{\mathrm{DOWN}}} = \frac{x_r}{L} \cdot \tilde{f}_{(m,i)} \tag{4.21}$$

where x_r is the distance that separates the i-th vehicle and the m-th RSU, while is the effective transmitting data rate for the link (i, m) (*uplink*), and (m, i) (*downlink*), respectively.

By adding the contribution of (4.21), we give the definition of v_{V2I} as the message propagation rate for communications between vehicles and RSUs via V2I protocol, such as

$$v_{\mathrm{V2I}} = v_{\mathrm{UP}} + v_{\mathrm{RSU}} + v_{\mathrm{DOWN}} = \frac{1}{L}\left[d \cdot B + x_r \cdot \left(\tilde{f}_{(i,m)} + \tilde{f}_{(m,i)}\right)\right]. \tag{4.22}$$

As an analogy, we can assume v_{V2V} as the message propagation rate for communications between vehicles by V2V protocol, such as

$$v_{\mathrm{V2V}}^{(\pm)} = \pm\left(v + c\right) = \pm\left(\frac{1}{hL}\sum_{i,j} x_{(i,j)} \cdot f_{(i,j)} + c\right), \tag{4.23}$$

which considers the contribution of (4.17). The positive or negative sign of c depends on the message propagation direction (*e.g.*, if a vehicle is moving at speed c along the opposite message propagation direction, the message propagation rate will be $-c$).

Then, it follows:

$$\begin{cases} v_{\mathrm{V2V}}^{(+)} = \frac{1}{hL}\sum\limits_{i,j} x_{(i,j)} \cdot f_{(i,j)} + c, \\ v_{\mathrm{V2V}}^{(-)} = -\frac{1}{hL}\sum\limits_{i,j} x_{(i,j)} \cdot f_{(i,j)} - c, \end{cases} \tag{4.24}$$

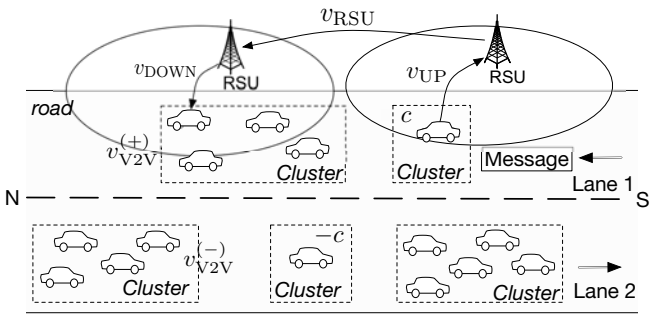


Figure 4.11: Velocity of message propagation in different phases of routing with V2X protocol.

Finally, when no connectivity occurs (*i.e.*, a vehicle is traveling alone in the highway), the message propagation rate is a constraint equal to $\pm c$ (again, the message propagation direction affects the positive or negative sign of c).

Figure 4.11 shows the message propagation rates for different transmission ways in V2X protocol, by assuming the message propagation direction is the north.

We can characterize the behavior of the whole system in terms of six transition states, such as:

1. Messages are traveling along on a vehicle in the N direction, at speed c;
2. Messages are propagating multi-hop within a cluster in the N direction, at speed $v^{(+)}_{\text{V2V}}$;
3. Messages are traveling along a vehicle in the S direction, at speed $-c$;
4. Messages are propagating multi-hop within a cluster in the S direction, at speed $v^{(-)}_{\text{V2V}}$;
5. Messages are transmitted via radio by an RSU in the N direction, at speed v_{V2I};

6. Messages are transmitted via radio by an RSU in the S direction, at speed $-v_{\mathrm{V2I}}$.

States (1-4) are typical for data propagation with opportunistic networking techniques in VANET scenarios where vehicles communicate only via V2V [62], while state 5, and 6, have been added for vehicles communicating via V2I. All the six states are available for V2X protocol.

As illustrated in [62], the *bridging* technique is strongly employed in opportunistic networking for vehicular networks, in order to avoid disconnections. In VANETs, there are two message propagation directions, such as the forward and reverse propagation. In forward message propagation, each vehicle is assumed to be traveling along the N direction at speed c [m/s], and also the message is propagated in the N direction.

The message propagation rate has a minimum value due to the speed of the vehicle (*i.e.*, c [m/s]), since the message is traveling along the vehicle. When a connection between two consecutive vehicles traveling in the N direction is available, the message will be propagated via V2V at a rate $v_{\mathrm{V2V}}^{(+)}$.

Moreover, if no vehicle connection is available, the bridging technique can attempt to forward a message to some clusters along the S (opposite) direction, whenever they are overlapping with the cluster along the N direction [62]. In this case, for bridging technique, the forward message propagation rate will be in the range $[c, v_{\mathrm{V2V}}^{(+)}]$, depending on the cluster size on the S direction.

In contrast, when a vehicle is communicating via V2I protocol, the forward message propagation rate is in the range $[c, v_{\mathrm{V2I}}]$. Analogously, in reverse message propagation, a message could be forwarded by vehicles traveling in an opposite direction respect to the

message propagation. In this case each vehicle is assumed to be traveling along the S direction at speed $-c$ [m/s], and also the message is propagated in such direction. When a connection between two consecutive vehicles traveling in the S direction is available, the message will be propagated via V2V at a rate $v_{\mathrm{V2V}}^{(-)}$.

When no vehicle connection is available, a message will be forwarded to some clusters along the N (opposite) direction, similarly to bridging technique in forward message propagation.

It follows that the reverse message propagation rate for vehicles communicating via V2V will be in the range $[-c, v_{\mathrm{V2V}}^{(-)}]$, depending on the cluster size on the S direction; while for vehicles communicating via V2I protocol, the reverse message propagation rate is in the range $[-c, v_{\mathrm{V2I}}]$.

4.7.1 Message Propagation Algorithm

After defining the message propagation rates in the VANET scenario, where vehicles can communicate via V2V or V2I, we introduce an algorithm for message propagation with V2X protocol.

The algorithm is based on the *Infrastructure Connectivity* (IC) parameter, which gives information if a vehicle can be connecting to a neighboring RSU. As a reminder, if a vehicle has IC = 0, no neighboring RSUs are available; otherwise, it means the vehicle is crossing one or more wireless cells (*i.e.*, IC = 1).

The proposed message propagation algorithm works the following tasks:

1. *Checking IC*: this phase is addressed to every source/relay vehicle. Every time a

vehicle is sending, or receiving a message, it will check its IC parameter. If a vehicle has IC = 1, it will send the message directly to the neighboring RSU via V2I; otherwise, the vehicle will forward the message to other vehicles via V2V, if they are available;

2. *Forwarding propagation*: this phase is addressed to every source/relay vehicle. A source/relay vehicle sends the message in the same message direction via V2V, if there is connectivity;

3. *Communication via V2I*: after the Checking IC phase, if the value of IC is equal to 1, then the vehicle will be start the initialization and instauration of a V2I link with an RSU;

4. *Tracking the destination vehicle(s)*: this phase is addressed to every RSU that receives a message. The RSU can know the destination vehicle's position (*i.e.* by A-GPS technology). If the destination vehicle is traveling within the RSU's wireless coverage, the RSU is going to send the message directly to the destination vehicle. Otherwise, if the destination vehicle is not in the RSU's wireless coverage, the RSU will be connecting the RSU that is actually managing the vehicle's connectivity, and will send the message to it. Finally, the new RSU will send the message directly to the destination vehicle.

The pseudo-code is depicted in Algorithm 1. The algorithm accepts one input (*i.e.* the vehicle's IC), and returns the actual vehicular communication protocol (*i.e.* $\{v_{\text{V2V}}, v_{\text{V2I}}\}$). All the phases of the algorithm are illustrated, and collected on the basis of different tasks

of each vehicle (*i.e.*, source, and relay vehicles), and RSU.

In summary, we consider that the switching protocol decision is just performed on the basis of local information, and the value of IC parameter.

Let us assume a source vehicle A is communicating with other vehicles via V2V in a sparsely connected neighborhood, where the transmission range distance between two consecutive vehicles is under the connectivity bound (*i.e.* $x < 125$ m, [88]). The vehicle A is not inside a wireless network (*i.e.* IC $= 0$). A destination vehicle B is driving far away from A, and other vehicles (relay) are available to communicate each other.

Every time a vehicle is forwarding a message, it will check its IC parameter. When IC $= 1$, the vehicle is crossing a wireless cell, and will calculate the optimal path according to (4.12), in order to send the message directly to the selected RSU via V2I. Otherwise, the vehicle will forward the message to neighboring vehicles via V2V. Then, the RSU knows the destination vehicle's position (*i.e.* by A-GPS). If the destination vehicle is traveling within the RSU's wireless coverage, the RSU will send the message directly to the destination vehicle. Otherwise, the RSU will be simply forwarding the message to the RSU that is actually managing the vehicle's connectivity. Finally, the message will be received by the destination vehicle.

Input:

IC Infrastructure Connectivity,

Output:

v_{V2V}, if the vehicle communicates via V2V,

v_{V2I}, if the vehicle communicates via V2I.

while IC = 0 **do**
| A vehicle is connected via V2V, $\leftarrow v_{\mathrm{V2V}}$

end

else

| **if** IC = 1 **then**
| | Detect the optimal path, $\leftarrow v_{\mathrm{V2I}}$
| **end**

end

if *a vehicle is in* v_{V2I} **then**
| RSU tracks the destination's position
| **if** *Destination vehicle is inside the RSU's coverage* **then**
| | Direct link from RSU to B
| | **else**
| | | RSU will forward the message to an RSU nearby.
| | **end**
| **end**

end

Algorithm 1: Protocol switching decisions in V2X.

4.7.2 Simulation results

As a measure of performance, we calculate the average message propagation rate according to the proposed algorithm, for different traffic conditions. We show the maximum and the minimum bounds of the message displacement (*i.e.*, x [m]), obtained for vehicles communicating via V2X.

In each of six states illustrated in Section 4.7, a message propagates with certain rate and the message displacement in the network scenario is a function of time (*i.e.*, $x(t)$), such as:

1. The message displacement for a message traveling along on a vehicle in the N direction is $c \cdot t$;

2. The message displacement for a message propagating multi-hop within a cluster in the N direction is $v_{\mathrm{V2V}}^{(+)} \cdot t$;

3. The message displacement for a message traveling along a vehicle in the S direction is $-c \cdot t$;

4. The message displacement for a message propagating multi-hop within a cluster in the S direction is $v_{\mathrm{V2V}}^{(-)} \cdot t$;

5. The message displacement for a message transmitted via radio by an RSU in the N direction is $v_{\mathrm{V2I}} \cdot t$;

6. The message displacement for a message transmitted via radio by an RSU in the S direction is $-v_{\mathrm{V2I}} \cdot t$.

We simulated a typical network scenario by the following events:

- at $t = 0$ s a source vehicle is traveling in the N direction. Its IC parameter is 0. A message is traveling along on the source vehicle (state 1);
- at $t = 3$ s the source vehicle enters in a RSU's radio coverage and its IC parameter is 1. The message is being transmitted via V2I to the RSU, then transmitted via radio by the RSU in the N direction, until it will be sent to the destination node at $t = 10$ s (state 5).

We compared this scenario where the message propagation algorithm has been employed, with traditional opportunistic networking in VANET, where vehicles can communicate only via V2V [62].

In this case, the events that represent such scenario are:

- at $t = 0$ s a source vehicle is traveling in the N direction. A message is traveling along on the source vehicle (state 1);
- at $t = 4$ s the message is forwarded to a vehicle in the S direction (state 3);
- at $t = 6$ s the message is propagating via multi-hop within a cluster in the N direction (state 2), until it will reach the destination node at $t = 10$ s.

For comparative purposes, in the simulation setup we have posed some parameters according to [62], and [93] such as $c = 20$ [m/s], and $d = 500$ [m]. Typical message size $L = 300$ [bit], data rate transmission $B = 10$ [Mbit/s] (*e.g.* for WiMAX base stations), and $x_r = 400$ [m] have been assumed. The transmission rates have been assumed as

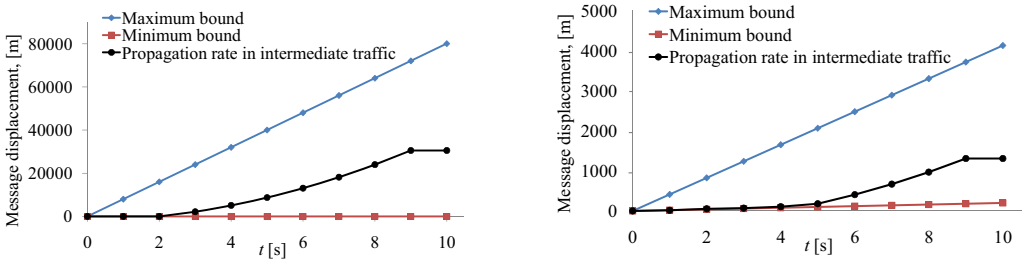


Figure 4.12: Forward message propagation with (*left*) V2X protocol, (*right*) traditional opportunistic networking.

$f_{(i,m)} = f_{(m,i)} = 5$ [Mbit/s], and $f_{(i,j)} = 2$ [kbit/s]. For each hop in a cluster (*i.e.* $h = 5$) we considered different distances between couples of vehicles (*i.e.*, 100, 50, 75, 40, and 30 m).

The performance of message propagation with V2X protocol is compared with traditional dissemination algorithm used in VANET [62]. Figure 4.12 (*left*) depicts the maximum and minimum message propagation bounds, for V2X protocol in a forward message propagation mode. It represents a message that is traveling along the same vehicle direction (see Figure 4.11).

Analogously, a message could be forwarded in reverse message propagation by vehicles traveling in an opposite direction. In this case, the data propagation rate is $-c$ [m/s], when data are traveling along a vehicle on the S direction; in multi-hop, a cluster along the S direction achieves a propagation rate of $-(c + v)$ [m/s].

By introducing the heterogeneous network infrastructure in traditional VANETs, we can notice a strong increasing of the message propagation with the V2X protocol, with respect to the traditional opportunistic networking (see Figure 4.12 (*right*)).

Figure 4.12 (*left*) depicts the maximum/minimum message propagation bounds for V2X

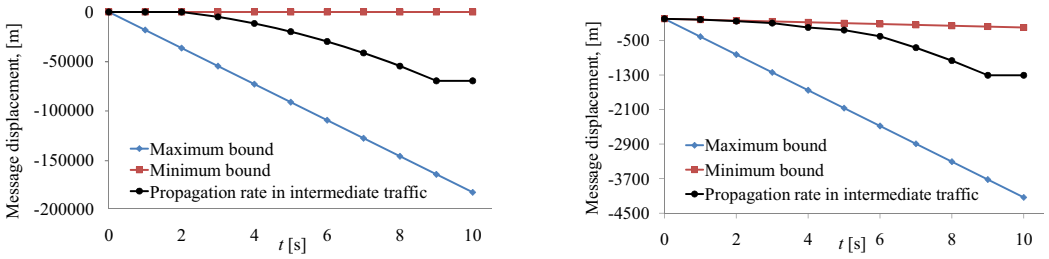


Figure 4.13: Reverse message propagation with (*left*) V2X protocol, (*right*) traditional opportunistic networking.

protocol, and the simulated scenario in *forward message propagation* mode. It represents a message that is traveling along the same vehicle direction (see Figure 4.4). We notice a strong increasing of the message propagation, with respect to the traditional opportunistic networking: after $t = 10$ s, the message has been propagating for around 50 km in V2X (Figure 4.12 (*left*)), while only 1.5 km in traditional V2V (Figure 4.12 (*right*)). This is due to the protocol switching decision of V2X, which exploits high data rates from network infrastructure.

Analogously, a message could be forwarded in *reverse message propagation* by vehicles traveling in an opposite direction (Figure 4.13 (*left*)). In this case, the data propagation rate is $-c$ [m/s], when data are traveling along a vehicle on the S direction; in multi-hop, a cluster along the S direction achieves a propagation rate of $-(c+v)$ [m/s]. For the *reverse message propagation* in traditional opportunistic networking scheme the message propagation rate is in the range $[c, v_{\mathrm{V2V}}^{(-)}]$ [m/s] (see Figure 4.13 (*right*)). Also in *reverse message propagation* case, V2X assures high values (*i.e.* at $t = 10$ s, messages have been propagated up to 70 km), while traditional V2V can achieve low values (*i.e.* at $t = 10$ s,

messages have reached 1.3 km far away from the source vehicle).

Small fluctuations of message displacement in *forward* and *reverse* cases with V2X (*i.e.* 50, and 70 km) depend on traffic density, and RSU positions.

As a conclusion, in this Section we described a hybrid vehicular communication protocol V2X and the mechanism by which a message can be propagated under this technique. In scenarios where vehicles communicate via V2X, we have characterized the upper and lower bounds for message propagation rates. Simulation results have shown how the V2X protocol improves the network performance with respect to traditional opportunistic networking technique applied in VANETs.

4.8 Satellite links in VANETs

The last Section of this Chapter deals with the introduction of satellite links in traditional VANETs. This novel safety service for VANETs represents an open issue to analyze. Preliminary results shown in [9] will be depicted in this Section.

Satellite radio is one of a complementary set of network connectivity technologies in future vehicles equipped with *on-board* computers. As previously said, other technologies include Bluetooth, Wi-Fi, WiMAX, UMTS, and DSRC. Collectively these technologies can enable V2V, and V2I connectivity, but under different operating conditions.

When a vehicle is driving alone in an area that is devoid of telephony infrastructure area (*i.e.*, a rural area during night hours), or it is in a disaster and emergency situation, a satellite network can provide service connection.

In this Section we briefly introduce the relationship between satellite radio connectiv-

ity, and other opportunistic connectivity schemes that rely on short-range communication applied in VANETs. We also describe an opportunistic vehicular networking scheme for safety applications, based on satellite communication links (*i.e.*, LEO/MEO satellite constellations).

In such scenario (see Figure 4.14 (*left*)), a vehicle (called as *isolated vehicle*) is driving alone on the road (*i.e.*, the traffic density reaches the minimum value), and no radio coverage (*e.g.*, no Wi-Fi access points, or cellular base stations). The isolated vehicle seeks to send an SOS message to any neighboring vehicle to alert about an accident occurred. The SOS message (where the vehicle's position is stored) is sent to the satellite in view (*i.e.*, LEO/MEO satellite constellations) by the vehicle (uplink connection).

The satellite receives the SOS message, processes the vehicle's position information, and forwards the message to ground by spot coverage.

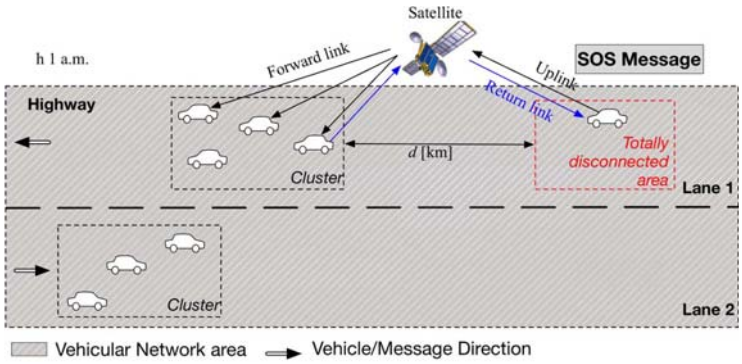


Figure 4.14: Novel opportunistic networking scheme in VANET scenario, with satellite connectivity for safety applications.

Consequently, the SOS message will be forwarded to the cluster of vehicles, closest to the isolated source vehicle ("forward link"). When the cluster of vehicles receives the SOS

message, it will send an acknowledgment (return message) to the satellite in visibility, which forwards it to the isolated vehicle ("return link").

The proposed scheme shows how the satellite connectivity can solve the problem of seamless and ubiquitous connectivity, when a vehicle is driving alone in an isolated area. The satellite works as "bridge", in order to connect the vehicle to the closest cluster of vehicles, driving in an urban area.

A physic layer analysis has been addressed in order to evaluate (*i*) the minimum distance among cluster of vehicles and isolated user vs. satellite orbit (LEO/MEO tradeoff), (*ii*) the service availability along a selected time window (*e.g.*, from 0 a.m. to 6 a.m.), (*iii*) the LEO/MEO satellites visibility from uplink and downlink coverage ("End-to-End" visibility), (*iv*) link feasibility and availability (*i.e.*, "End-to-End" Signal-to-Noise and Interference ratio), (*v*) forward and return link delay, and payload dimensioning. An example of visibility analysis for MEO constellation (*i.e.* Galileo) is reported in Figure 4.15.

Our technique is intended to augment short and medium-range communication to bridge isolated vehicles or clusters of vehicles when no other mechanism is available.

Particular, each vehicle should be equipped by GNSS Receiver, and by Ka Tx/Rx. The GNSS Rx provides information about (*i*) the number of Satellites Supporting Vehicles (SSV) in visibility, and (*ii*) the isolated vehicle's position. Ka Tx/Rx permits the link with the MEO SSV.

The main steps of our safety application by satellite link are as follows:

1. An isolated vehicle transmits a message to transparent SSV in visibility by Ka1 band Tx antenna (Forward Link –*uplink*), (see Figure 4.16 (*a*));

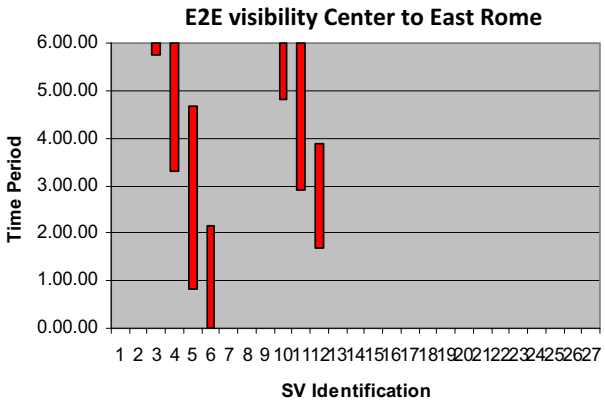


Figure 4.15: Forward link End-to-End (E2E) visibility, Rome city vs. East Rome.

2. SSV forwards at Ka2 band to ground by spot coverage (Forward Link –*downlink*). A cluster of cars/Ground Service provider receives the forwarded distress message (see Figure 4.16 (*b*));

3. An acknowledgement message is transmitted by GNSS system (Return Link) (see Figure 4.16 (*c*));

4. User receives the acknowledgement, (see Figure 4.16 (*d*));

5. Transmission is concluded.

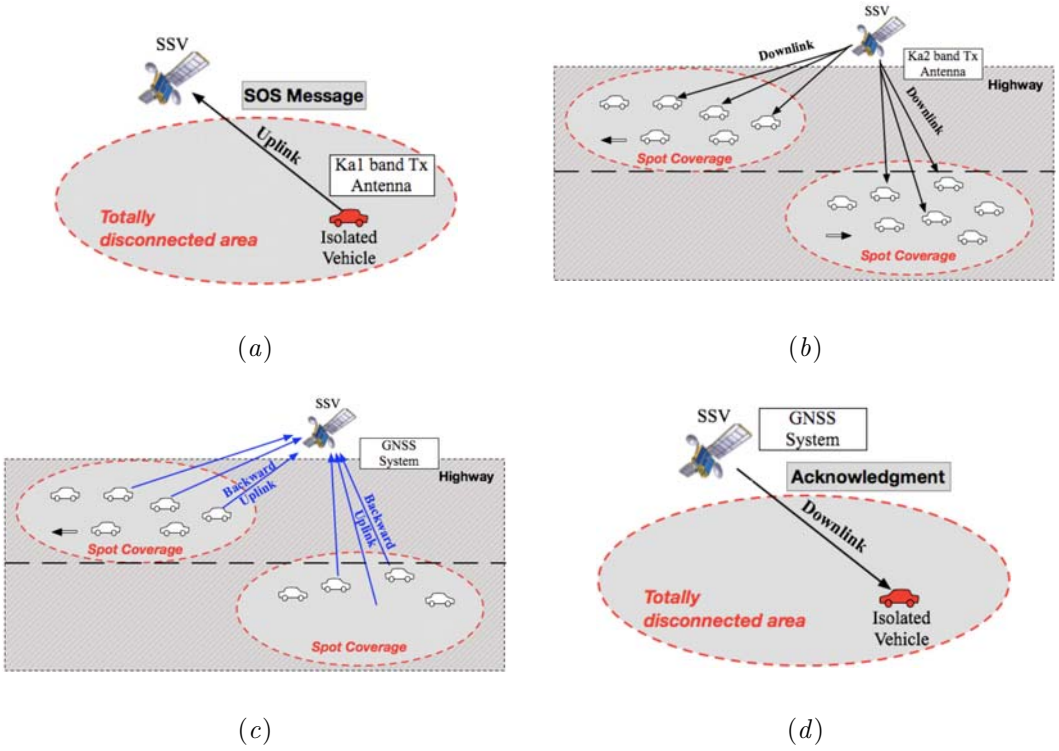


Figure 4.16: Forward (a) uplink, and (b) downlink. Backward (c) uplink, and (d) downlink.

4.9 Conclusions

A novel hybrid protocol for vehicular communications has been proposed. Based on a switching protocol decision metric, V2X determines which protocol (V2V or V2I) to employ for a vehicle driving in a particular network scenario (*i.e.*, dense, and sparse traffic scenario). By introducing the preexistent network infrastructure (*i.e.*, wireless and cellular networks), the traditional vehicular network has been improved in a HWN scenario.

We have also defined an optimal path selection technique, and evaluated the total cost

function metric. Simulation results show which protocol between V2V and V2I gives best performance, for the two different network scenarios. V2I performance depends on the data rate over a direct link to an RSU, while V2V performance is strictly depending on the number of hops that composes a path. Finally, V2X represents a dynamic communication protocol for vehicular networking, due to fast protocol switching actions, and is depending on traffic density, radio resource utilization time and delay factor.

Moreover, we have described a novel message propagation algorithm based on the hybrid V2X protocol for vehicular communications. The proposed protocol exploits both traditional V2V technique, and V2I, through the use of fixed infrastructure such as roadside units. In this scenario, we have characterized the upper and lower bounds for message propagation, and simulated performance behavior for a typical VANET traffic scenario. We have also illustrated an algorithm for a correct protocol switching decision in V2X.

Simulation results have shown how the V2X protocol improves the network performance with respect to traditional opportunistic networking technique applied in VANETs.

Finally, recent work is dealing with the introduction of satellite links for safety applications in VANETs [9].

Chapter 5

Local Positioning Indoor Services

5.1 Introduction

The location techniques are the basis of a new class of services, called as Location Based Services (LBS), providing appropriate contents to the user, to the right place and in the most simple and rapid way. An increasing number of mobile and smart phones allow people to access the Internet, wherever they are and whenever they want.

This new scenario includes a wide range of services based on the possibility to localize and track the user in a location-aided environment, such as emergency and rescue assistance, info-mobility, and so on. Reliable and accurate position information of mobile users is necessary by the adoption of the Federal Communications Commission (FCC) regulations to provide Enhanced-911 (E-911) service, [94]. According to Aktas and Hippenstiel [95], LBSs are information services accessible with mobile devices through the mobile network and utilizing the ability to make use of the information about the location of the mobile and cellular devices. At this aim, several techniques are used to localize non-cooperating cellular phones, as Time Differences of Arrival (TDOA) method, whose estimate is obtained

by the cross correlation between signals arriving at two base stations. So, localization of the wireless transmitter is solved by the intersection of two hyperbolic curves, [96]. Thus, an LBS represents an intersection of three technologies, such as Internet, mobile devices and Geographic Information Systems, [97]. LBSs provide a two way communication and interaction, according to actual user context, including his position. So, integration of localization services in wireless networks is an open issue, as actual satellite based location systems (*e.g.* GPS) are widely employed in the outdoor environment, but barely used in the indoor one.

In general, local positioning systems employ a grid of reference nodes that communicate with any mobile terminal, in order to determine either its range or the angles of the line of sight from the reference nodes to it, and then apply triangulation or trilateration algorithms to determine its locations. Several methods designed for IEEE 802.11, Bluetooth, and RFID networks estimate the MT distance based on the strength of the signals received by each reference node [98, 99]. However, these techniques perform rather poorly, since in complex environments the received signal is prone to fading induced by multipath. When high accuracy is required, either TOA or DOA has to be employed. At this aim, we extend the Basic Service Set topology of IEEE 802.11 networks, with a set of reference nodes that perform either TOA or DOA measurements, according the proposed Localization Services protocol. More specifically, the architecture consists of a grid of several Localization Supporting Nodes (LSNs) (*e.g.* 6 LSNs), and one Localization Supporting Server (LSS). The LSS whose position is known works as Point of Coordination. It estimates the position of a mobile terminal inside the IEEE 802.11a/g grid. The Location Supporting Nodes perform

TOA/DOA estimations, on the basis of localization packets sent by the mobile terminals.

The main tasks of the LSS are: registration of incoming MTs, distribution of synchronization signals, coordination of TOA/DOA measurements, TOA/DOA measurements collection, location estimate, and location notification. On the other hand, each LSN performs the TOA/DOA measures based on the location packets sent by the MTs. To support both measurement and broadcasting of the estimated MT position, we propose the joint use of both PCF (Point Coordination Function), and DCF (Distributed Coordination Function) IEEE 802.11 Medium Access Control (MAC) modes. As already mentioned, to reduce the coordination overhead, the LSS functionalities are normally provided by the AP that acts as Point Coordinator (PC) in PCF mode. In DCF mode the control is decentralized among peer nodes. Exploitation of the PCF mechanism allows to periodically update the location of each registered MT at a rate that depends on its mobility class, ensuring the agreed level of service, while avoiding typical DCF collisions. On the other hand, since the LSNs that are in the range of each MT are a priori unknown, use of DCF mode, for notification of the TOA/DOA measurements performed by them, is more efficient than polling. The LSS periodically broadcasts an advertisement, notifying all MTs that location services are supported by the network.

When a new MT enters the area served by an LSS, it sends to the LSS a location service registration request specifying its mobility class. The LSS inserts its identifier and mobility class (*i.e.* no mobility, low and high mobility), as well as other parameters such as registration lifetime, into the Location List and, then, sends a confirmation to the MT, specifying which mode (DOA, or TOA) is supported.

The registered MTs are periodically requested by the LSS, to activate the Location Updating procedure. Specifically, it consists of:

1. **Location Update Request (LUR)**: right after the BEACON packet at the beginning of a super-frame, the LSS sends an LUR (Location Update Request) packet to the next MT of the Location List whose position has to be update;

2. **Location Packet (LP) Broadcasting**: the MT replies to the LSS request by broadcasting a Location Packet during the CF_{UP} phase of the PCF (after a SIFS interval has been elapsed). The LP is received by the LSNs that are in the range of the MT. In TOA mode, the timestamp of the instant at which the packet has been sent is saved in a table of a local MT memory;

3. **MT-LSN location report**: each LSN that has successfully received the MT-LP sends back a report containing the information extracted by the LSN. More specifically, in TOA mode, the report contains the current LSN latency, given by the difference between the time-stamp of the instant at which it has received the LP, and the time-stamp of the instant at which the report is sent back to the MT. In DOA mode, this report contains the estimated direction of arrival measured by the LSN;

4. **LSN report collection**: in TOA mode, the MT collects the LSN location reports transmitted back by LSNs during the DCF phase. For each report the Time Sum of Arrival (TSOA) is extracted. As illustrated in Figure5.1, to weaken the requirement on temporal synchronization among nodes, the average range between the MT and each LSN is evaluated by means of the difference between the time elapsed from the

broadcast of the LP and the reception of the report, and the current LSN latency contained in the report itself. The actual ranges are then sent to the LSS by the MT. In DOA mode no special post processing is required, since LSNs directly provide the estimated DOAs;

5. **Location computation e updating**: the triangulation or the trilateration algorithm can be executed either by the MT itself or the LSS, depending on the computing capability of the MT. In the first case, the MT notifies to the LSS its new position. This solution reduces the overhead and the time needed to obtain the estimate. As a drawback, the location of the LSNs has to be broadcasted, for instance, in the Location Services Advertisement. In the second case the MT sends to the LSS a Location Update report containing the actual ranges or the DOAs. In principle, relay of DOA measurements from MT to the LSS can be avoided, when all LSNs are in the LSS range. Once received all the LSN estimates, the LSS computes the MT position. Depending on the Quality of Service class of the MT, the estimated location is either immediately sent to the MT, by means of a dedicated packet, or is pigged-back on the next LUR packet.

The overall process is repeated at multiples of the Shortest Location Update Interval, typically chosen as a multiple of the super-frame duration, based on the MT mobility class. Different users to be localized are distributed on different super-frames.

The position estimation is delayed to the next scheduled instant if necessary. The duration of the PCF phase is related to the number of registered MTs and then could be reduced by the LSS by broadcasting a CF_{END} packet.

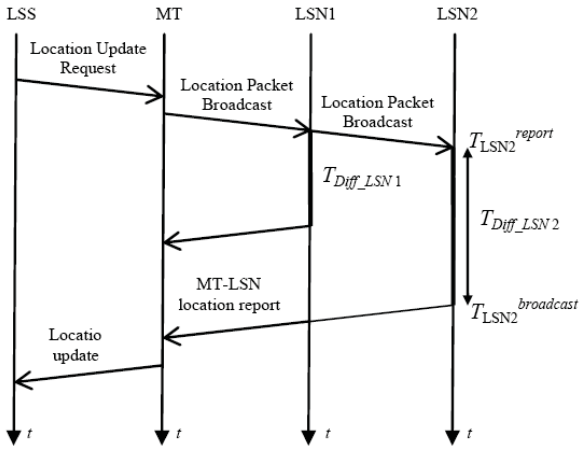


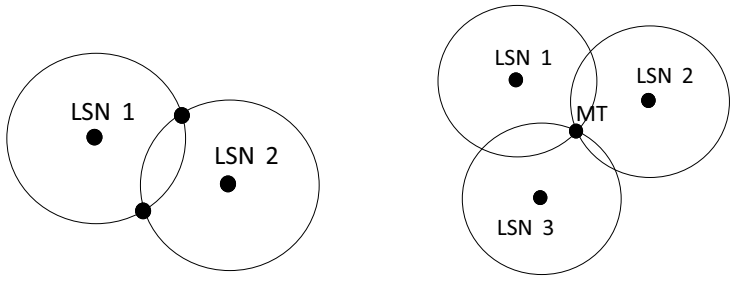
Figure 5.1: Packet Forwarding model for TOA mode.

5.2 TOA approach

The TOA system determines the MT position based on the intersection of the distance circles, also called as LSN ranges.

Assuming that the LSN positions are known to the LSS, two range measurements provide an ambiguous fix, while three measurements determine a unique position for MT in the horizontal plane, as represented in Figure 5.2(a) and 5.2(b), respectively. The same principle is used by GPS, by considering spheres as circles, and the fourth measurement to solve the receiver-clock bias for a 3D solution. Obviously, accuracy can be increased by using more TSOA, when available.

To reduce the impact of the location services on the Wi-Fi throughput, the LSNs could also be directly connected to the LSS by a wired LAN. In this case, MT location can be extracted by means of a multilateration performed on the TDOA of the LP, estimated on the basis of the TDOA of the LSN reports, compensated for the LSN latencies annotated



(a) Three measurements determine a unique position for MT.

(b) Ambiguous measurement for just two range measurements.

Figure 5.2: TOA position estimation method.

in the LSN reports themselves.

In TOA mode, since instantaneous bandwidth and typical Signal-to-Noise Ratio are high enough to warrant very accurate location, the main source of error is constituted by the reference time distribution. Since in GPS only a one-way communication from satellites to location devices is possible, time alignment is obtained by resorting to reference signal provided by atomic clocks. Here, we exploited the two-ways communication capability of the IEEE 802.11 networks to design a solution that imposes simpler constrains on the timing reference distribution. Obviously this approach requires a careful use of both MAC and physical layers of IEEE 802.11a/g.

In particular, as discussed in the previous paragraph, we use both IEEE 802.11 PCF and DCF modes to estimate and track the MT position at a rate selected according to the user speed. Since the range is estimated on the basis of the two-way time of flight from MT to LSN and vice versa, its accuracy is affected by the accuracy of the estimate of the Time of Departure (TOD) of a packet, as well as by the accuracy of the estimate of its

TOA. Since the sources of error can be considered independent, we can write the variance of ranging error as the sum of two contributions, such as

$$\sigma_R^2 = c^2 \left(\sigma_{TOD_{MT}}^2 + \sigma_{TOA_{LSN}}^2 + \sigma_{TOD_{LSN}}^2 + \sigma_{TOA_{MT}}^2\right) = 2c^2 \left(\sigma_{TOD}^2 + \sigma_{TOA}^2\right), \quad (5.1)$$

where c is the speed of the electromagnetic wave, σ_{TOD}^2 is the TOD error variance, and σ_{TOA}^2 is the TOA error variance. We observe that σ_{TOD}^2 is strictly related to the implementation of the transmitter timing, while σ_{TOA}^2 is related to the square of the effective bandwidth fe and to the Signal-to-Noise ratio (SNR) between the energy E_r of the received signal and the power spectral density N_0 of the receiver noise. Equation (5.1) shows that the Cramer Rao Low Bound (CRLB) is:

$$\sigma_{TOA}^2 \geq \left[8\pi^2 SNR \left(\frac{SNR}{1+SNR}\right) f_e^2\right]^{-1}, \quad (5.2)$$

where f_e is the effective bandwidth, expressed as:

$$f_e^2 = \frac{\int_{-W}^{W} f^2 \left|S\left(f\right)\right|^2 df}{\int_{-W}^{W} \left|S\left(f\right)\right|^2 df}, \quad (5.3)$$

with $S(f)$ the spectrum of the transmitted signal. In Figure 5.3 the CRLB on the contribution $\sigma'_R = \left(c\sigma_{TOA}\right)/\sqrt{2}$ to the standard deviation of the range error produced by the TOA error for a nominal bandwidth of 5 MHz and a flat signal spectrum is plotted. We notice that, to obtain a standard deviation of 20 cm, an SNR of about 38 dB is required.

Knowledge of the actual geometry allows to translate the variances of the errors of the available LSN ranges into the covariance matrix of the location error.

To achieve the Cramer Rao Lower Bound a coarse-to-fine estimator can be implemented, [100]. To reduce the computational complexity, the possibility of performing the

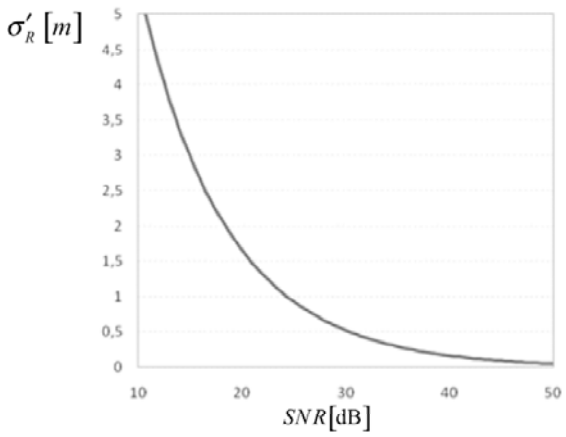


Figure 5.3: CRLB of the contribution to the standard deviation of the range error produced by the TOA error for a nominal bandwidth of 5 MHz.

fine TOA estimation by direct use of the data provided by the OFDM demodulator, employed in IEEE 802.11a/g, has been investigate by the authors. Since in IEEE 802.11a/g the spectrum of the received signal is directly available at the output of the OFDM receiver, the fine TOA estimate can be extracted from the linear phase shift between the Fourier transform of the transmitted and the received signals by means of a Kalman filter, as described below.

Let $s(t)$ be the transmitted signal by the MT, and $r(t) = s(t - \Delta t) + w(t)$ the signal received by the LSN, where $w(t)$ is an additive Gaussian noise. Then,

$$\begin{aligned} S^*(f)\,R(f) &= |S^*(f)\,R(f)|\,e^{-j\Delta\varphi(f)} \\ &= |S(f)|^2 e^{-j2\pi f\Delta t} + S^*(f)\,W(f)\,. \end{aligned} \tag{5.4}$$

The phase $\Delta\phi(f)$ di $S^*(f)R(f)$ can be written as:

$$\Delta\phi(f) = -2\pi f\Delta t + \nu(f) \tag{5.5}$$

where, for high values of signal-to-noise ratios SNR, $\nu(f)$ can be modeled as a sample of

a zero mean, white Gaussian noise. In IEEE 802.11a/g, $N = 52$ sub-carriers are employed, 48 of them reserved to data, and 4 to control data (*pilot*).

Thus, let $\Delta t(h)$ be the time delay corresponding to the h-th location packet of a given MT, and $\Delta\varphi_m(h)$ be the phase shift of the mth sub-carrier f_m for that packet, so that

$$\Delta\varphi_m(h) = -2\pi\Delta t(h) f_m + v_m(h), \quad m = 0, 1, ..., N-1. \tag{5.6}$$

We modeled the time delay variations induced by the user mobility with a first order, discrete time, dynamical system, driven by a white Gaussian noise, *i.e.*,

$$\Delta t(h+1) = \Delta t(h) + n(h). \tag{5.7}$$

For a faster DSP implementation, we can rearrange the dynamical (5.1) and (5.2), by introducing a parallel to serial conversion of the phase shift subcarrier array related to an OFDM symbol period. Therefore, by posing

$$\begin{cases} h = k \bmod N \\ m = k - hN \end{cases} \tag{5.8}$$

we obtain

$$z(hN + m) = \Delta\varphi_m(h), \tag{5.9}$$

or equivalently,

$$z(k) = -2\pi\Delta t\left[k - (k \bmod N)\right] f_{k \bmod N} + \nu(k). \tag{5.10}$$

In addition, we pose

$$a(hN + m) = \Delta t(h), \tag{5.11}$$

and we rewrite the time delay dynamical (5.2) as

$$a\left(k+1\right)=\begin{cases} a\left(k\right)+n\left(k\right), & k \bmod N=0 \\ a\left(k\right), & \text{otherwise} \end{cases} \tag{5.12}$$

Finally, we can rearrange the dynamical (5.3) as follows:

$$\begin{cases} a\left(k+1\right)=a\left(k\right)+\omega\left(k\right) \\ z\left(k\right)=-2\pi f_{k \bmod N}a\left(k\right)+\upsilon\left(k\right) \end{cases} \tag{5.13}$$

where $\upsilon(k)$ is a stochastic process that models the OFDM phase shift noise, and $\omega(k)$ is a white, zero mean, Gaussian stochastic process modeling the uncertainty produced by the MT mobility, whose covariance, by virtue of (5.7), is

$$R_{\omega}\left(k\right)=\begin{cases} \sigma_{\omega}^{2}, & k \bmod N=0 \\ 0, & \text{otherwise} \end{cases} \tag{5.14}$$

We see that $\sigma^2(\omega)$ is a function of the user mobility. In fact, let V_{max} be the user maximum speed, A_{Max} its maximum acceleration, and τ the time interval between two measurements, we can set $\sigma(\omega)$ equal to:

$$a\left(k+1\right)=a\left(k\right)+\omega\left(k\right).$$

Regarding $\upsilon(k)$, we modelled it as a white, zero mean, Gaussian process with covariance equal to the inverse of the receiver Signal-to-Noise Ratio (SNR):

$$\sigma_{\upsilon}^{2}=1/SNR. \tag{5.15}$$

Finally, the TOA estimate is represented by the output of Kalman filter corresponding to the last subcarrier of an OFDM symbol:

$$z\left(k\right)=-2\pi f_{k \bmod N}a\left(k\right)+\upsilon\left(k\right). \tag{5.16}$$

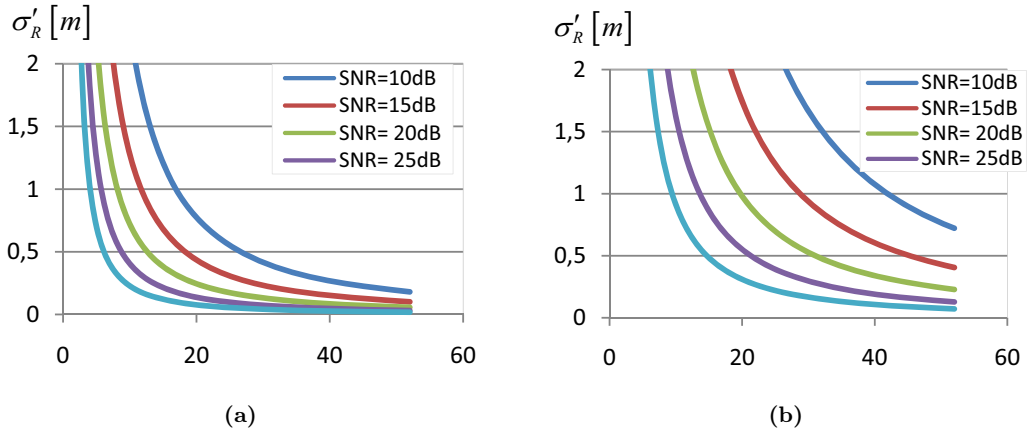


Figure 5.4: (a) Standard deviation of synchronization error, calculated for $f_e = 5$ MHz. (b) Standard deviation of synchronization error, calculated for $f_e = 20$ MHz.

For sake of compactness, the well known Kalman filter equations are omitted. In Figure 5.4(a) and 5.4(b) the contributions to the standard deviation of the range error produced by the TOA error, for 5 and 20 MHz of transmitter bandwidth, versus the Kalman Filter iterations corresponding to one OFDM symbol are reported. We note they are in good agreement with the CRLB.

For a more realistic evaluation of the performance, we simulated the use of the localization system, based on the TOA extraction in the OFDM domain, at the Applied Electronics Department of University of "Roma TRE" (see Figure 5.5). The whole area was partitioned into several zones, each with an LSS and several LSNs. For each path, 100 Monte Carlo runs have been done. The nominal isotropically radiated power density at a range of 1m from the transmitter was set to -40 dBm, while the receiver noise level was set to -100 dBm. The channel attenuation losses L_{loss} versus the distance D were computed as $L_{loss} = \gamma log_{10} D$, where the attenuation exponent γ was randomly generated

in the range $[1.5, 3]$, accordingly to the channel impulsive response measures performed in the same environment.

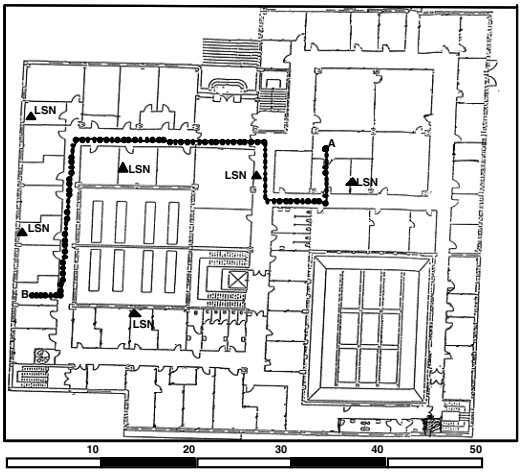


Figure 5.5: Map of the Applied Electronics Department and geometry of the simulated MT's path.

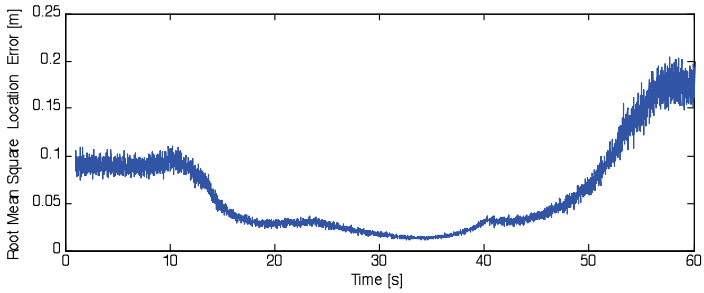


Figure 5.6: Root mean square position error vs. simulation time.

Figure 5.6 shows the position estimation uncertainty caused by a one-way TOA measure, along the path from A to B depicted in Figure 5.5, served by 6 IEEE 802.11a LSNs employing a 20 MHz bandwidth. The simulation results are in good agreement with the theoretical performance of Figure 5.4(a), and 5.4(b). They demonstrate the feasibility of

indoor location services based on IEEE 802.11 networks. In Figure 5.5, high values of the root mean square location error depend on the radio coverage guaranteed by only two LSNs, (*i.e.* LSN1 and LSN6), at the end of the path. The least error occurs at $t = 36$ s, when the MT moves in a part of the building covered by several LSNs, (*i.e.* LSN2, LSN3, and LSN4).

In principle, TSOA gives the average MT range with respect to two different instants. Moreover, since in IEEE 802.11 networks the maximum TOA is of the order of 0.3μs, the main source of error is constituted by latency. Nevertheless, for speeds up to 10 m/s, as those expected in indoor applications, even a latency of 5 ms produces errors less than 2.5 cm.

5.3 DOA approach

The main drawback of the TOA-based methods is represented by the need of precisely synchronized clocks for the transmitters and receivers. So, a timing misalignment between the LSSs directly results in a position estimation error, as Figure 5.7 depicts.

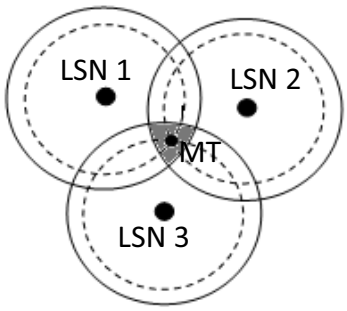


Figure 5.7: TOA timing errors. Grey area represents the uncertain region for MT position.

At subunit level, the main difference in the implementation of TOA and DOA, is consti-

tuted by the LSN antenna array, as in DOA the angle of arrival is extracted by processing the snapshots of the space-time field. The DOA scheme utilizes adaptive antenna arrays together with sophisticated DOA processing. Mobile users can be located, in the horizontal plane, when a minimum of two DOA estimates are established. The MT position can be determined by finding the intersection of the corresponding bearing lines.

In Figure 5.8 the intersection of two directional Lines Of Bearing (LOB) defines a unique position, each formed by a radial from a LSN to the MT in a two-dimensional space. The DOA scheme utilizes adaptive antenna arrays together with sophisticated DOA processing. Mobile users can be located, in the horizontal plane, when the minimum of two DOA estimates are established at multiple LSNs. The position locating results in a trigonometric type of problem that can be worked out by finding the coordinates from the intersection of two or more LOB. In this way, the MT's position is determined by the following formulas:

$$\begin{cases} p = (x_2 - x_1) \cdot \frac{\sin(\alpha)\sin(\beta)}{\sin(\beta-\alpha)}, \\ q = \frac{p}{\tan(\alpha)} = (x_2 - x_1) \cdot \frac{\cos(\alpha)\sin(\beta)}{\sin(\beta-\alpha)}. \end{cases} \tag{5.17}$$

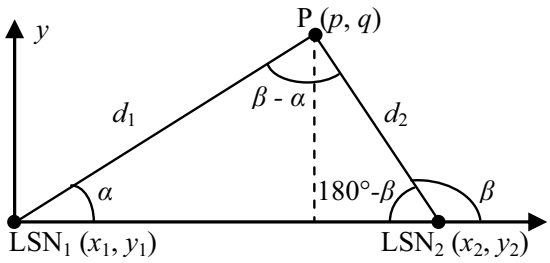


Figure 5.8: DOA position estimation method for a pair of LSNs, each of them has a LOB from the MT's position.

Let us recall that the variance σ_{ψ}^2 of the DOA estimate is related to the number of elements M_A composing the array through the Cramer Rao lower bound for wavenumber vector that for linear arrays is, [101] p. 980.

$$\sigma_{\psi}^2 \geq \frac{6}{\left(M_A^2 - 1\right) M_A} 2W \left(\frac{N_0}{E_r}\right), \tag{5.18}$$

where W is the signal bandwidth, N_0 is the power spectral density of the receiver noise, and E_r is the energy of the received signal. For a given geometry, the covariance matrix of the location error can then be computed from the variance of each DOA estimate as illustrated, for example, in [102, 103].

Obviously, estimation accuracy improves when a higher number of measures (*i.e.* LoBs) are utilized, but at the cost of increasing computational complexity. In [104] a possible candidate for LSN antenna is presented, working at 2.4 GHz, according to IEEE 802.11 requirements. Figure 5.9 shows the proposed antenna design for IEEE 802.11a/g technology.

Antenna electrical design has been performed by commercial electromagnetic 3D software. Antenna has been tested by HP 8510 Network analyzer for the *s*-parameters, and by anechoic chamber for the radiation pattern and polarization purity.

The antenna is designed to work at 5.0 GHz in broadband mode in RHCP; however, by a proper dimensioning of the slots, resonating frequencies can be steered, so the antenna can work in dual frequency mode [105]. Respect to a "standard" patch antenna the proposed single element appears more compact (effect of the slots on the resonating frequencies).

Antenna is matched on the wireless operating frequencies and the percentage is more than 8% (1 : 1.5 VSWR) considering $f = 5.0$ GHz as the centre frequency. The polarization

purity is less than −25 dB at boresight, −20 dB at the edge of coverage [−15°; +15°]. More details are illustrated in [104], and [106].

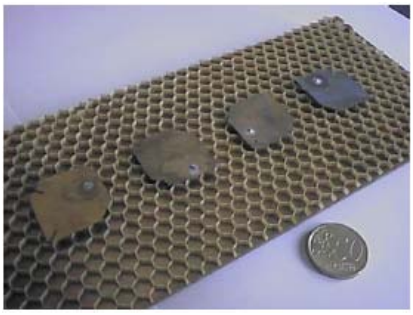


Figure 5.9: Microstrip antenna array for LSN and LSS, 5 cm × 18 cm × 2 cm.

5.3.1 Protocol Performance

The performance of the localization services protocol have been investigated by analyzing, at first, the maximum number of MTs that can be served with a predefined fraction of the throughput, [98]. At this aim, we observe that, in the worst case, the time interval necessary to poll a user at the maximum distance $r_{\max}$, to broadcast a location packet and then to calculate the user position, as:

$$T = 2\frac{r_{\max}}{c} + 2T_{SIFS} + \frac{D_{LUR} + D_{ACK}}{B}, \tag{5.19}$$

where $r_{\max}$ is the maximum distance served by the LSS [m], c is the speed of light [m/s], T_{SIFS} is the SIFS interval duration, D_{LUR} is the LUR packet size [bit], D_{ACK} is the LP size [bit], and B is the Data Rate [bit/s]. Thus, the number of users that the system is able to manage within one super-frame (PCF+DCF) is given by

$$N = \frac{\Delta T_{PCF_{\max}} - T_{SIFS} + \frac{D_{BEACON} + D_{CF_{END}}}{B}}{T + \varepsilon\left(\frac{r_{\max}}{c} + \frac{D_{LUR}}{B} + T_{PIFS}\right)}, \tag{5.20}$$

where $\Delta T_{PCF\max}$ is the maximum duration of the PCF [ms] interval assigned to the localization services, D_{BEACON} is the BEACON packet size [bit], $D_{CF_{END}}$ is the CF_{END} packet size [bit], T_{PIFS} is the PIFS interval duration, and ϵ is the performance reduction factor due to the coverage area and channel noise.

By considering (5.19) and (5.20), the maximum number of users the network is able to manage is,

$$N_{TOT} = \frac{\Delta T_{POLL}}{\Delta T_{SUPERFRAME}} \cdot \frac{1}{\Im(N)}, \tag{5.21}$$

where ΔT_{POLL} is the polling period of the same MT, $\Delta T_{SUPERFRAME}$ is the super-frame duration, and $\Im(N)$ is the integer part of N. As stated previously, N_{TOT} is strictly related to the LUR time and hence to the mobility class of the users.

Figure 5.13 shows the maximum number of users that can be located, for different values of data rates and LSN range. We note that our localization algorithm can localize a minimum value of 100 users for 6 Mbit/s, and a maximum value of 250 over 36 Mbit/s. To evaluate the performance, we simulated a multiple mobile terminal scenario with 6 LSNs located on the hexagon vertexes and one LSS in the hexagon center.

The coverage area was set to the maximum distance between the LSN and the LSS. According to IEEE 802.11 standard, the size of data packet used to poll the MTs was fixed to 400 bit and the ACK packet size to 112 bit. Slowly moving MTs with maximum speed of 2 m/s were considered.

Consequently, the time interval between location updates was set to 0.5 s. Data rate from 6 to 26 Mbps have been considered, while the LSS coverage area was set to the maximum value specified by the IEEE 802.11 standard for the specific data rate in indoor

environment. For each case different paths have been simulated, varying the MT initial position and motion direction, in order to collect the statistics of at least 1000 different points of the grid.

From the simulator outputs the Location Update Waiting Time (LUWT), lasting from the instant at which the LSS queries the MT to the time the MT receives back the LSN estimates was computed, together with the average number of available LSNs in the MT range and the number of LSNs actually employed. Finally, the location probability expressed as the probability that the LSS receives at least three measures, was evaluated.

Respectively, Figure 5.10, 5.11, and 5.12 depict the LUWT, the number of LSNs used, and the Location Probability as function of the number of MTs for four different data rate/coverage area values, respectively.

Figure 5.10 shows that the LUWT increases as soon as the number of MTs increases. The main cause for that is the increasing number of collisions. On the other hand, the number of used LSN decreases, since the LSNs have to send longer packets (containing more TOA/DOA estimations) during the DCF phase, causing an additional increase in the number of collisions (see Figure 5.11). These figures show that to achieve better performance it is more important to have a higher coverage area rather than a higher data rate.

Finally, from Figure 5.12 it turns out that with a probability greater than 80%, the LSS receives at least three distance measures for each of the 25 MTs for LSN coverage areas greater than 25 m, while the number of localizable MTs drops to 10 for coverage areas less than 25 m.

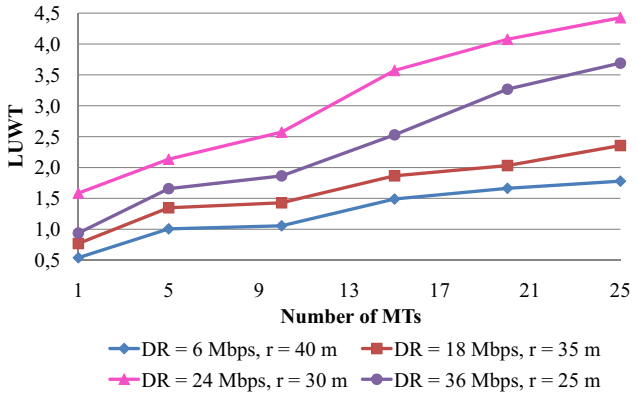


Figure 5.10: Location Update Waiting Time vs. number of MTs.

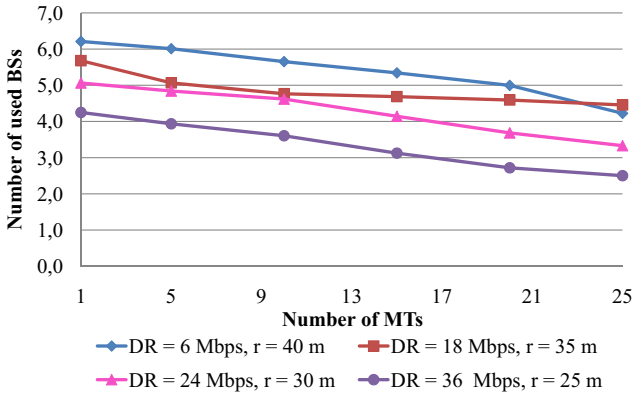


Figure 5.11: Number of used LSNs vs. number of MTs.

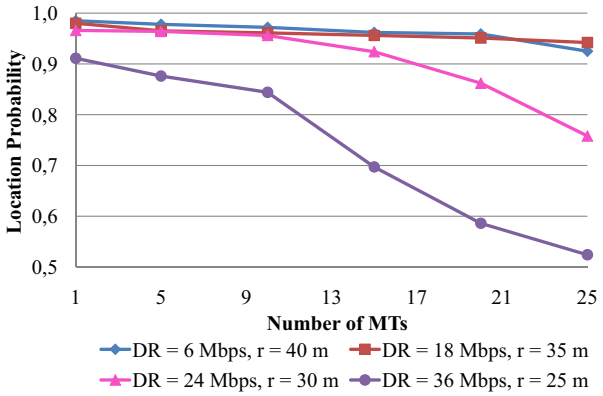


Figure 5.12: Location Probability vs. number of MTs.

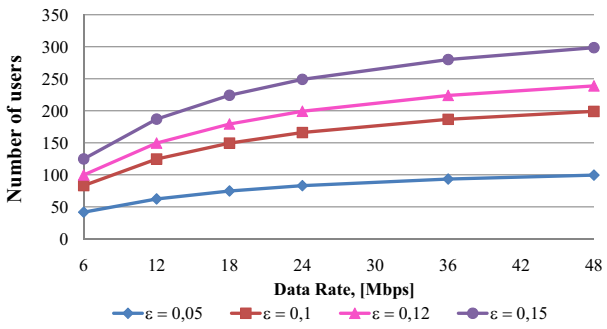


Figure 5.13: Number of users, for $\Delta T_{SUPERFRAME} = 5$ ms.

Chapter 6

Acknowledgment

In the first place I would like to record my gratitude to my supervisor Prof. Alessandro Neri for his high quality supervision, advice, and guidance from the very early stage of my research, as well as giving me extraordinary experiences through out the work. Without his help, this work would not be possible. Above all and the most needed, he provided me encouragement and support in various ways, and for any doubt and problem I had. His truly scientist intuition has made him as a constant point of reference, and enriched my growth as a student, and now as Doctor of Philosophy.

I am very grateful to my co-advisor Prof. Thomas D.C. Little for his constant support and for giving me the opportunity to work at his Multimedia Communication Laboratory, in Boston University, Boston, MA. The experience spent in Boston was the best opportunity for my academic carrier, I could ever be expecting. Prof. Little enriched my knowledge with his exceptional insights into many aspects of vehicular networks.

I also want to thank Prof. Gaetano Giunta for his huge availability, and for giving me the opportunity to collaborate in his teaching activity at University of Roma Tre.

I gratefully acknowledge Prof. Roberto Cusani for his advices, supervision, and crucial contribution. Collaboration at University of Rome Sapienza was a very profitable deal. Sapienza is for me my second university in Rome. Many thanks go in particular to Tiziano Inzerilli, who was one of first person who taught me how to make research in vertical handover between wireless networks.

I am also grateful to Prof. Francesco Vatalaro, Marco Leo and all other people working at RadioLabs, for their valuable advices in science discussion, and supervision. My experience in RadioLabs during the Project sponsored by TiLab was a very interesting work.

Then, a special thanks to Prof. Ibrahim Matta, and Flavio Esposito (Ph.D. Student at Boston University, Computer Science Department). Meeting Flavio has been a second gift I received in Boston, after having the opportunity to work with Prof. Little. I want to thank Flavio for his technical assistance, and fun during the work we had in Boston, and still now via email and on Skype calls.

My special thanks go to all my friends in Rome and those I met in Boston, who made me feel at home, though being far away from Rome.

Lastly, I would like to thank my parents for their daily support and patience during my nervous moments. My father and mother always gave me assistance and great advises when I needed. Moreover, I am greatly indebted to my brother Claudio, who now I should also call as “collegue”, due to many papers we wrote together.

Finally, thanks also to an old friend of mine who encouraged and suggested me to spend a research period in USA, in particular in Boston.

Bibliography

[1] T. Inzerilli and A.M. Vegni. "A reactive vertical handover approach for WiFi-UMTS dual-mode terminals". In *Proc. of 12th Annual IEEE Int. Symposium on Consumer Electronics (ISCE 2008)*, Vilamoura (Portugal), April 14-16, 2008.

[2] T. Inzerilli, A.M. Vegni, A. Neri, and R. Cusani. "A Location based Vertical Handover algorithm for limitation of the ping-pong effect". In *Proc. of 4th IEEE Int. Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2008)*, Avignon (France), October 12-14, 2008.

[3] A.M. Vegni, G. Tamea, T. Inzerilli, and R. Cusani. "A Combined Vertical Handover Decision Metric for QoS Enhancement in Next Generation Networks". In *Proc. of 5th IEEE Int. Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2009)*, Marrakech (Morocco), October 12-14, 2009.

[4] G. Tamea, A.M. Vegni, T. Inzerilli, and R. Cusani. "A Probability based Vertical Handover Approach to Prevent Ping-Pong Effect". In *Proc. of 6th International Symposium on Wireless Communication Systems 2009 (ISWCS 2009)*, Siena (Italy), September 7-10, 2009.

[5] A.M. Vegni and F. Esposito. "A Speed-based Vertical Handover Algorithm for VANET". In *Proc. of 7th International Workshop on Intelligent Transportation (WIT 2010)*, Hamburg, Germany, March 23-24, 2010.

[6] P.G. Bosco, T. Inzerilli, M. Leo, and A.M. Vegni. "Extended UPnP architecture for emergency applications". In *Proc. of Wireless Rural Emergency Communications Conference (WRECOM 2007)*, Roma (Italy), October 1-3, 2007.

[7] A.M. Vegni, T.D.C. Little, and A. Neri. "Vehicle-to-X Protocol for Vehicular Networking". Submitted to *EURASIP Journal on Advances in Signal Processing*, Special Issue on "Vehicular Ad Hoc Networks", 2010.

[8] A.M. Vegni and T.D.C. Little. "A Message Propagation Algorithm in V2X Protocol". Submitted to *Proc. of 2nd International Workshop on Communication Technologies for Vehicles (Nets4Cars 2010)*, July 21-23, 2010, Newcastle, UK.

[9] A.M. Vegni, C. Vegni, and T.D.C. Little. "Opportunistic Vehicular Networks by Satellite Links for Safety Applications". Accepted presentation at Fully Networked Cars Workshop @ Geneva Motor Show, Geneva (Swizerland), March 3-4, 2010.

[10] IEEE 802.21 Media Independent Handover Services -Media Independent Handover, Draft Text for Media Independent Handover Specification.

[11] V. Gupta, M.G. Williams, D.J. Johnston, S. McCann, P. Barber, and Y. Ohba. "IEEE 802.21 Overview of Standard for Media Independent Handover Services", July 2006.

[12] N. Golmie, U. Olvera-Hernandez, R. Rouil, R. Salminen, and S. Woon. "Imple-

menting Quality of Service based handovers using the IEEE 802.21 framework", July 2006.

[13] M. Montenovo, A. Perot, M. Carli, P. Cicchetti, and A. Neri. "Objective quality evaluation of video services". In *Proc. on Second International Workshop on Video Processing and Quality Metrics (VPQM)*, Scottsdale, AZ, January 15-16, 2006.

[14] A. Neri, M. Carli, M. Montenovo, A. Perrot, and F. Comi. "No reference quality assessment of Internet multimedia services". In *Proc. on 14th European Signal Processing Conference (EUSIPCO-2006)*, Florence, Italy, September 4-8, 2006.

[15] J. Shin, J. W. Kim, and C.-C. J. Kuo. "Quality-of-Service Mapping Mechanism for Packet Video in Differentiated Services Network". *IEEE Transactions on Multimedia*, 3,(2), June, 2001.

[16] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. High-speed Physical Layer in the 5 GHz Band, 1999.

[17] F. Siddiqui and S. Zeadally. "Mobility management across hybrid wireless networks: Trends and challenges". *Computer Communications*, 29, 2006.

[18] J. Laiho, A. Wacker, and T. Novosad. *Radio Network Planning and Optimisation for UMTS*. 2nd edition, December 2005. Chapter 3, pp. 95-98.

[19] H.D. Cho, et al. "A study on the MCHO method in Hard handover and Soft handover between WLAN and CDMA". In *Proc. on International Conference on Consumer Electronics, (ICCE 2005)*, pages 391–392, January 8-12, 2005.

[20] A.M. Vegni, M. Carli, A. Neri, and G. Ragosa. "QoS-based Vertical Handover in Heterogeneous Networks". In *Proc. of 10th Int. Symposium on Wireless Personal Multimedia Communications (WPMC 2007)*, Jaipur (India), December 3-6, 2007.

[21] K. Yang, I. Gondal, B. Qiu, and L. S. Dooley. "Combined SINR based vertical handoff algorithm for next generation heterogeneous wireless networks". In *Proc. on IEEE Global Telecommunications Conference, GLOBECOM'2007.*, Washinton, DC, USA, November 26-30, 2007.

[22] M.R. Kibria, A. Jamalipour, and V. Mirchandani. "A location aware three-step vertical handoff scheme for 4G/B3G networks". In *Proc. on IEEE Global Telecommunications Conference, GLOBECOM'2005*, volume 5, St. Louis, MO, USA, 28 Nov. - 2 Dec. 2005.

[23] N. Zhang and J.M. Holtzman. "Analysis of handoff algorithms using both absolute and relative measurements". *IEEE Transactions on Vehicular Technology*, 45(1):174–179, February 1996.

[24] S.S. Wang, M. Green, and M. Malkawi. "Adaptive Handoff Method Using Mobile Location Information". In *Proc. on IEEE Emerging Technology Symposium on Broadband Communications for the Internet Era*, pages 97–101, Sept. 2001.

[25] A. Markopoulos, P. Pissaris, S. Kyriazakos, C. Dimitriadis, G. Karetsos, and E.D. Sykas. "Increased Handover Performance in 2G and 3G Wireless Systems Based on Combined Mobile-Location and Area". In *Proc. on IEEE International Symposium*

on Wireless Personal Multimedia Communications, volume 1, pages 47–51, October 2002.

[26] D.B. Lin, R.T. Juang, H.P. Lin, and C.Y. Ke. "Mobile Location Estimation Based on Differences of Signal Attenuations for GSM Systems". In *Proc. on IEEE Soc. Int. Conf. Antennas and Propagation*, number 1, pages 77–80, June, 2003.

[27] T. Inzerilli, A.M. Vegni, A. Neri, and R. Cusani. "A Location and Power Management Based Hybrid Approach for Vertical Handover Decision and Mobile Controlled Connectivity". Submitted to IEEE Transactions on Vehicular Technology, 2010.

[28] J. McNair and Z. Fang. "Vertical Handoffs in fourth-generation Multinetwork Environments". *IEEE Wireless Communications*, 11(3):8–15, June, 2004.

[29] H. Bing, C. He, and L. Jiang. "Performance analysis of vertical handover in a UMTS-WLAN integrated network". In *Proc. of IEEE Int. Symposium on Personal, Indoor and Mobile Radio Communications*, volume 1, pages 187–191, September, 2003.

[30] A. Hasswa, N. Nasser, and H. Hossanein. "Generic Vertical Handoff Decision Function for Heterogeneous Wireless". In *Proc. on 2nd IFIP Int. Conf. on Wireless and Optical Communications Networks, WOCN 2005*, pages 239–243, March 6-8, 2005.

[31] H. Holma and A. Toskala. *WCDMA for UMTS*. John Wiley, New York, 2004.

[32] S. Toumpis and A. J. Goldsmith. "Capacity regions for wireless ad hoc networks". *IEEE Transactions on Wireless Communications*, 2,(4), July, 2003.

[33] X. Cai and C. Chi. "An Analytical Model for Performance Evaluation of Handover

Decision Algorithms". In *Proc. on 2nd International Conference on Communications and Networking in China, CHINACOM 2007*, pages 1079–1083, August 22-24, 2007.

[34] Y. Fang and I. Chlamtac. "Analytical generalized results for handover probability in wireless networks". *Trans. on IEEE Communications*, 50(3):396–399, March, 2002.

[35] C. Chi, X. Cai, R. Hao, and F. Liu. "Modeling and Analysis of Handover Algorithms". In *Proc. on IEEE Global Telecommunications Conference (GLOBECOM 2007)*, pages 4473–4477, Washington, DC, USA, November 26-30, 2007.

[36] H. Moustafa and Y. Zhang (Eds.). *Vehicular Networks: Techniques, Standards and Applications.* Auerbach publishers, Taylor & Francis Group, 2009.

[37] G. Held. *Inter- and intra-vehicle communications.* CRC Press, November 08, 2007. ISBN 9781420052213.

[38] O. Tonguz, N. Wisitpongphan, F. Bai, P. Mudalige, and V. Sadekar. "Broadcasting in VANET". In *Proc. on Mobile Networking for Vehicular Environments*, pages 7–12, Anchorage, AK, May 2007.

[39] S. Balasubramaniam and J. Indulska. "Vertical Handover Supporting Pervasive Computing in Future Wireless Networks". *Computer Communication Journal, Special Issue on 4G/Future Wireless Networks*, 27(8):708?719, 2003.

[40] Z. Yan, H. Zhou, H. Zhang, and S. Zhang. "Speed-Based Probability-Driven Seamless Handover Scheme between WLAN and UMTS". In *Proc. on 4th International*

Conference on Mobile Ad-hoc and Sensor Networks, pages 110–115, Los Alamitos, CA, USA, 2008. IEEE Computer Society.

[41] D. Kwak, J. Mo, and M. Kang. "Investigation of handoffs for IEEE 802.11 networks in vehicular environment". In *Proc. on First Int. Conference on Ubiquitous and Future Networks, ICUFN 2009*, pages 89–94, Hong Kong, June 7-9, 2009.

[42] Y.S. Chen, C.H. Cheng, C.S. Hsu, and G.M. Chiu. "Network Mobility Protocol for Vehicular Ad Hoc Network". In *Proc. on IEEE Wireless Communications and Networking Conference (WCNC 2009)*, Budapest, Hungary, April 5-8, 2009.

[43] J.A. Olivera and I. Cortázar and C. Pinart and A. Los Santos and I. Lequerica. "VANBA: a simple handover mechanism for transparent, always-on V2V communications". In *Proc. on IEEE 69th Vehicular Technology Conference (VTC2009-Spring)*, April 26?29 2009.

[44] J. Guo, R. Yim, T. Tsuboi, and J. Zhang. "Fast Handover Between WiMAX and WiFi Networks in Vehicular Environment". In *World Congress and exhibition on Intelligent Trasport Ssytems and Services*, September, 2009.

[45] "Recommendation ITU-R M.1225: Guidelines for evaluation of radio transmission technologies for IMT-2000". Technical report, 1997.

[46] F. Esposito, A.M. Vegni, I. Matta, and A. Neri. "Dad, slow down, I am watching the movie – On Modeling Speed-Based Vertical Handovers in VANETs". submitted to MobiHoc 2010, the 11th ACM SIGMOBILE International Symposium on Mobile Ad Hoc Networking and Computing,, February 2010.

[47] R. Martì, J. Delgado, and X. Perramon. "Security Specification and Implementation for Mobile e-Health Services ". In *Proc. on the 2004 IEEE Int. Conf. on e-Technology, e-Commerce and e-Service (EEE-04)*, pages 241 – 248, March, 28-31 2004.

[48] A. Meissner, T. Luckenbach, T. Risse, T. Kirste, and H. Kirchner. "Design challenges for an integrated disaster management communication and information system". In *1st IEEE Workshop of Disaster Recovery Networks (DIREN 2002)*, June 24, 2002.

[49] `http://openvpn.net/`.

[50] Markus Feilner. *OpenVPN: Building and Integrating Virtual Private Networks*. Packt Publishing Ltd.

[51] `http://www.upnp.org/`.

[52] M.C. Chan, H. Hadama, and R. Stadler. "An Architecture for Broadband Virtual Networks under Customer Control". *IEEE NOMS,*, April, 1996.

[53] `http://jaxta.org/`.

[54] Brendon J. Wilson. *"Jaxta Book"*. New Riders, June 2002.

[55] `http://osgi.com/`.

[56] *"OSGi Service Platform: The OSGi Alliance"*. IOS Press, (hardcover) release 3, edition, 2003.

[57] S. Kent and R. Atkinson. *"Security Architecture for the Internet Protocol"*. November, 1998. IETF RFC2401.

[58] K. Egevang and P. Francis. The IP Network Address Translator (NAT), May 1994.

[59] *Intel Authoring Tool for UPnP Technologies, Intel ®Corporation, 2003.*

[60] *Intel Development Tools for Implementing UPnP Devices, Intel ®Corporation, 2003.*

[61] *UPnP AV Architecture:0.83, ©1999-2000 Contributing Members of the UPnP Forum, 2002.*

[62] T.D.C. Little and A. Agarwal. "An information propagation scheme for VANETs". In *Proc. on 8th Intl. IEEE Conf. on Intelligent Transportation Systems (ITSC 2005)*, pages 155–160, September 13-16, 2005.

[63] USP researchers say future cars will communicate to avoid collisions. Available online: `http://www.usp.ac.fj/news/story.php?id=416`.

[64] A. Agarwal and T.D.C. Little. "Impact of Asymmetric Traffic Densities on Delay Tolerant Vehicular Networks". In *Proc. of 1st IEEE Vehicular Networking Conference (VNC-2009)*, Tokyo (Japan), October 28-30, 2009.

[65] "Wireless Access in Vehicular Environments (WAVE) Networking Services, IEEE 1609.3/D15", 2006.

[66] X. Ma, X. Chen, and H.H. Refai. "Performance and Reliability of DSRC Vehicular Safety Communication: A Formal Analysis". *EURASIP Journal on Wireless Communications and Networking, Speical issue on Wireless Access in Vehicular Environments*, (3):13, January 2009.

[67] T.K. Mak, K.P. Laberteaux, and R. Sengupta. "A multi-channel VANET providing concurrent safety and commercial services". In *Proc. of 2nd ACM International Workshop on Vehicular Ad Hoc Networks, (VANET 2005)*, Cologne (Germany), September 2, 2005.

[68] J. Santa, A. Moragon, and A.F. Gomez-Skarmeta. "Experimental evaluation of a novel vehicular communication paradigm based on cellular networks". In *Proc. on IEEE Intelligent Vehicles Symposium*, pages 198–203, Eindhoven (Netherlands), June 4-6, 2008.

[69] C-C. Hung, H. Chan, and E.H-K. Wu. "Mobility pattern aware routing for heterogeneous vehicular networks". In *Proc. on IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2200–2205, Las Vegas NV, 31 March-3 April, 2008.

[70] J. Miller. "Vehicle-to-Vehicle-to-Infrastructure (V2V2I) Intelligent Transportation System architecture". In *Proc. on IEEE Intelligent Vehicles Symposium*, pages 715–720, Eindhoven (Netherlands), June 4-6, 2008.

[71] J. Zhu and S. Roy. "MAC for Dedicated Short Range Communication in Intelligent Transportation System". *Topics in Wireless Communication, IEEE Communication Magazine*, December 2003.

[72] IEEE Draft P1609.0/D01, 2007.

[73] IEEE Draft P802.11p/D2.0, November 2006.

[74] K. Fall. "A Delay-Tolerant Network Architecture for Challenged Internets". In *Proc. of Special Interest Group on Data Communications (ACM SIGCOMM'03)*, pages 27–34, Karlsruhe (Germany), August 25-29, 2003.

[75] P. Jacquet, B. Mans, and G. Rodolakis. "Information propagation speed in Delay Tolerant Networks: Analytic upper bounds". In *Proc. of IEEE International Symposium on Information Theory (ISIT 2008)*, pages 6–11, Toronto, Ontario (Canada), July 2008.

[76] H. Moustafa and Y. Zhang (Eds.). *Vehicular Networks: Techniques, Standards and Applications*. Auerbach publishers, Taylor and Francis Group, 2009.

[77] J. Ott and D. Kutscher. "Drive-thru Internet: IEEE 802.11b for automobile users". In *Proc. on IEEE INFOCOM 2004, 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 1, pages 361–373, March 7-11, 2004.

[78] X. Dong, K. Li, J. Misener, P. Varayia, and W. Zhang. "Expediting Vehicle Infrastructure Integration (EVII)". Technical report, California PATH Research Report, UCB-ITS-PRR-2006-20, 2006.

[79] L. Pelusi, A. Passarella, and M. Conti. "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks". *IEEE Communications Magazine*, 44(11):134–141, November 2006.

[80] G. Resta, P. Santi, and J. Simon. "Analysis of multihop emergency message propagation in vehicular ad hoc networks". In *Proc. on the 8th ACM international Sympo-*

sium on Mobile Ad Hoc Networking and Computing, (MobiHoc 2007), pages 140–149, Montreal, Quebec, (Canada), September 9-14, 2007.

[81] H. Jiang, H. Guo, and L. Chen. "Reliable and Efficient Alarm Message Routing in VANET". In *Proc. on the 28th International Conference on Distributed Computing Systems Workshops*, pages 186–191, 2008.

[82] S. Yousefi, M. Fathy, and A. Benslimane. "Performance of beacon safety message dissemination in Vehicular Ad hoc NETworks (VANETs)". *Journal of Zhejiang University Science A*, 2007.

[83] W. Chen, R.K. Guha, T.J. Kwon, J. Lee, and Y.Y. Hsu. "A survey and challenges in routing and data dissemination in vehicular ad hoc networks". In *IEEE Int. Conf. on Vehicular Electronics and Safety*, Columbus, OH, USA, September 22-24, 2008.

[84] T. Nadeem, P. Shankar, and L. Iftode. "A Comparative Study of Data Dissemination Models for VANETs". In *Proc. on the 3rd Annual International Conference on Mobile and Ubiquitous Systems (MOBIQUITOUS 2006)*, pages 1–10, San Jose, (California), July 17-21, 2006.

[85] M. Gerla, B. Zhou, F. Soldo, Y. Lee, G. Marfia, and U. Lee. "Vehicular Grid Communications: The Role of the Internet Infrastructure". In *Proc. on Wireless Internet Conference (Wicon 2006)*, Boston, MA, USA, August 3, 2006.

[86] G. Marfia, G. Pau, E. Giordano, E. De Sena, and M. Gerla. "Evaluating Vehicle Network Strategies for Downtown Portland: Opportunistic Infrastructure and Importance of Realistic Mobility Models". In *Proc. of MobiOpp 2007, Co-located with*

the ACM-USENIX International Conference on Mobile Systems, Applications, and Services, Porto Rico, (USA), June 11, 2007.

[87] A. Agarwal and T.D.C. Little. "Access Point Placement in Vehicular Networking". In *Proc. on 1st International Conference on Wireless Access in Vehicular Environments (WAVE)*, Troy, MI, December, 2008.

[88] A. Agarwal and T.D.C. Little. "Access Point Placement in Vehicular Networking". In *Proc. of 1st International Conference on Wireless Access in Vehicular Environments (WAVE)*, Dearborn (Michigan), USA, December 8-9, 2008.

[89] A.A. Kherani, D. Kumar, and E. Altman. "A Structural Property of Solutions to Path Optimization Problems in Random Access Networks". In *Proc. on 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, pages 1–6, Boston, MA, April 3-6, 2006.

[90] A. Pentland, R. Fletcher, and A. Hasson. "DakNet: Rethinking Connectivity in Developing Nations". *IEEE Computer*, 37(1):78–83, January, 2004.

[91] L. Pelusi, A. Passarella, and M. Conti. "Beyond MANETs: Dissertation on Opportunistic Networking". Technical report, IIT-CNR Tech. Rep.,, May 2006. online available at $http://bruno1.iit.cnr.it/\ andrea/tr/commag06_tr.pdf$.

[92] X. Ma, X. Chen, and H.H. Refai. "Performance and Reliability of DSRC Vehicular Safety Communication: A Formal Analysis". *EURASIP Journal on Wireless Communications and Networking*, page 13, 2009.

[93] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter. "Analytical Models for Information Propagation in Vehicle-to-Vehicle Networks". In *Proc. on ACM VANET*, Philadelphia, USA, October, 2004.

[94] FCC Report and Order and Further Notice of Proposed Rule Making. Technical Report FCC Docket No. 94-102, July 1996.

[95] U. Aktas and R. Hippenstiel. "Localization of GSM signals based on fourth order moment wavelet denoising". In *33rd Annual Asilomar Conference on Signals, Systems, and Computers*, volume 1, pages 457–461, 1999.

[96] K. Virrantaus, J. Markkula, A. Garmash, and Y. V. Terziyan. "Developing GIS-supported location based services". In *Proc. of 1st International Workshop on Web Geographical Information Systems (WGIS 2001)*, Kyoto (Japan), 2001.

[97] N. Shiode, C. Li, M. Batty, P. Longley, and D. Maguire. *The impact and penetration of location based services.* Telegeoinformatics: location-based computing and services, CRC Press, 2004.

[98] A. Di Nepi, G. Massaro, M. Carli, and A. Neri. "MAC location services for IEEE 802.11 networks". In *Proc. on IEEE 5th International Conference on Networking (ICN'06)*, Mauritius, April 23-29, 2006.

[99] C. Savarese, J.M. Rabaey, and J. Beutel. "Location in distributed ad-hoc wireless sensor networks". In *Proc. on IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'01)*, volume 4, Salt Lake City, UT, USA, 2001.

[100] H.L. Van Trees. *Optimum array processing. Detection, estimation and modulation theory, Part III.* New York: Wiley, 1968.

[101] H.L. Van Trees. *Optimum array processing. Detection, estimation and modulation theory, Part III.* New York: Wiley, 2002.

[102] A.G. Dempster. "Dilution of precision in angle-of-arrival positioning system". *IEEE Electronics Letters*, 42(5), March, 2006.

[103] D.H. Kim, S. Hun, and T. Sung. "Error Analysis of Time-Based and Angle-Based Location Methods". *Journal of Control, Automation and System Engineering*, 12(10):962–967, October 2006.

[104] A.M. Vegni, A. Di Nepi, A. Neri, and C. Vegni. "Localization services on IEEE 802.11 Networks". In *Proc. of 19th Int. Conference on Applied Electromagnetics and Communications (ICECom 2007)*, Dubrovnick (Croatia), September 24-26, 2007.

[105] K. L. Wong. *Compact and Broadband Microstrip Antennas.* John Wiley & Sons, Inc., New York, 2002.

[106] A. Neri, A.M. Vegni, and A. Di Nepi. TOA and DOA-based localization services in IEEE 802.11 networks. *ATTI dell'Istituto Italiano di Navigazione (I.I.N.)*, No. 187, January/February 2008.