TESIS DE LA UNIVERSIDAD
DE ZARAGOZA

2013

29

Domenico Sicignano

Analysis, evaluation and improvement of RT-WMP for real-time and QoS wireless communication: applications in confined environments

Departamento

Informática e Ingeniería de Sistemas

Director/es

Tardioli, Danilo
Villarroel Salcedo, José Luis

ISSN 2254-7606

Prensas de la Universidad
Universidad Zaragoza

Universidad Zaragoza
1542

Tesis Doctoral

ANALYSIS, EVALUATION AND IMPROVEMENT OF RT-WMP FOR REAL-TIME AND QOS WIRELESS COMMUNICATION: APPLICATIONS IN CONFINED ENVIRONMENTS

Autor

Domenico Sicignano

Director/es

Tardioli, Danilo
Villarroel Salcedo, José Luis

UNIVERSIDAD DE ZARAGOZA
Informática e Ingeniería de Sistemas

2013

PhD Thesis

Analysis, evaluation and improvement of RT-WMP for real-time and QoS wireless communication. Applications in confined environments

Domenico Sicignano

Supervisores:

José Luis Villarroel

Danilo Tardioli

Grupo de Robótica, Percepción y Tiempo Real
Departamento de Informática e Ingeniería de Sistemas
Escuela de Ingeniería y Arquitectura
Universidad de Zaragoza

Febrero 2013

PhD Thesis

Analysis, evaluation and improvement of RT-WMP for real-time and QoS wireless communication. Applications in confined environments

Domenico Sicignano

Febrero 2013

Supervisores:

José Luis Villarroel

Danilo Tardioli

Grupo de Robótica, Percepcióon y Tiempo Real
Departamento de Informática e Ingeniería de Sistemas
Escuela de Ingeniería y Arquitectura
Universidad de Zaragoza

PhD Thesis

Analysis, evaluation and improvement of RT-WMP for real-time and QoS wireless communication. Applications in confined environments

Domenico Sicignano

Febrero 2013

Supervisors

José Luis Villarroel	Universidad de Zaragoza
Danilo Tardioli	Centro Universitario de Defensa

Jury

Luis Montano	Universidad de Zaragoza
Luis Almeida	Universidade do Porto, Portugal
Carlos Sagües	Universidad de Zaragoza
Michael Gonzalez Harbour	Universidad de Cantabria
Marisol Garcia	Universidad Carlos III de Madrid

Ai mie genitori
e ai miei fratelli.

Io ritornai da la santissima onda
rifatto sì come piante novelle
rinnovellate di novella fronda,
puro e disposto a salire a le stelle.
(Dante Alighieri, Purgatorio Canto XXXIII)

Project framework

The work of this thesis has been developed with the Robotics, Perception and Real Time Group of the Universidad de Zaragoza, in the framework of the national projects NERO (DPI2006-07928), SICRA (TSI-020100-2010-384), TESSEO (DPI2009-08126) and the European Commission project URUS (EC IST-1-045062-URUS-STP). The thesis author also belongs to the Instituto de Investigación de Ingeniería de Aragón (I3A).

Here follows a short description of the cited project in chronological order:

NERO NEtworked RObots

The complex nature of mobile robot tasks leads to the necessity of systems with several coordinated robots (agents) working in cooperation. Some international directives refer to robotic elements connected to the communication nets or wireless nets including the robots themselves and the sensors distributed in the working place (static agents) exchanging and sharing information. This concept is extended to robot interactions between humans, the sensors and the environment. We propose this project which is very related with previous MEC projects obtained by this research team, to continue working on subjects related to multi-robot cooperation techniques, computer vision, robot vision for motion and communications.

URUS Ubiquitous Networking Robotics in Urban Settings

European cities are becoming difficult places to live due to noise, pollution and security. Moreover, the average age of people living European cities is growing and in a short period of time there will be an important community of elderly people. City Halls are becoming conscious of this problem and are studying solutions, for example by reducing the free car circulation areas. Free car areas imply a revolution in the planning of urban settings, for example, by imposing new means for transportation of goods, security issues, etc. In this project we want to analyze and test the idea of incorporating a network of robots (robots, intelligent sensors, devices and communications) in order to improve life quality in such urban areas.

SICRA Manegement system for avalanches rescues based on cooperative networks

The SICRA project considers the conception, developement and validation of a management system of rescue for snow avalanche victims in a real environment. SICRA suggests combining mesh networks systems (based on Zigbee protocols or s imilar over IEEE 802.15.4 technologies), GPS and assisted in communications geolocation, creating a expert system in order to help the rescue and integration teams with a control center that could help them to manegement and plan the actions in an optim way.

TESSEO TEams of robots for Service and Security missiOns

The project proposes to investigate techniques for a multi-robot team to act in coordination in realistic scenarios. For the deployment, it is necessary to deal with algorithms and methods related to task planning and allocation, coordinated navigation planning, environment perception from multiple views provided by every member of the team, while the communication connectivity among all the elements of the system is maintained – robots, infrastructure, supervisor team, etc. Although some of the techniques involved are usually proposed in the literature and in many projects somehow independently, the research in this project will also be oriented to develop techniques integrating the different subjects involved. Only in this way it will be possible to develop realistic applications using systems with autonomous and supervised behaviours.

Resumen

En los ultimos años, la innovación tecnológica, la característica de flexibilidad y el rapido despligue de las redes inalámbricas, han favorecido la difusión de la redes móviles ad-hoc (MANETs), capaces de ofrecer servicios para tareas específicas entre nodos móviles. Los aspectos relacionados al dinamismo de la topología móvil y el acceso a un medio compartido por naturaleza hacen que sea preciso enfrentarse a clases de problemas distintos de los relacionados con la redes cableadas, atrayendo de este modo el interés de la comunidad cientifica.

La redes ad-hoc suelen soportar tráfico con garantía de servicio mínimo y la mayor parte de las propuestas presentes en literatura tratan de dar garantías de ancho de banda o minimizar el retardo de los mensajes. Sin embargo hay situaciones en las que estas garantias no son suficientes. Este es el caso de los sistemas que requieren garantias mas fuertes en la entrega de los mensajes, como es el caso de los sistemas de tiempo real donde la pérdida o el retraso de un solo mensaje puede provocar problemas graves. Otras aplicaciones como la videoconferencia, cada vez más extendidas, implican un trafico de datos con requisitos diferentes, como la calidad de servicio (QoS). Los requisitos de tiempo real y de QoS añaden nuevos retos al ya exigente servicio de comunicación inalámbrica entre estaciones móviles de una MANET.

Además, hay aplicaciones en las que hay que tener en cuenta algo más que el simple encaminamiento de los mensajes. Este es el caso de aplicaciones en entornos subterráneas, donde el conocimiento de la evolución de propagación de la señal entre los diferentes nodos puede ser útil para mejorar la calidad de servicio y mantener la conectividad en cada momento.

A pesar de esto, dentro del amplio abanicos de propuestas presente en la literatura, existen un conjunto de limitaciones que van da el mero uso de protocolos simulados a propuestas que no tiene en cuenta de entornos no convencionales o que resultan aisladas desde el punto de vista de la integracion en sistemas complejos.

En esta tesis doctoral, se propone un estudio completo sobre un plataforma inalámbrica de tiempo real, utilizando el protocolo RT-WMP capaz de gestionar trafico multimedia al mismo tiempo y adaptado al entorno de trabajo. Se propone una extensión para el soporte a los datos con calidad de servicio sin limitar las caractaristicas temporales del protocolo básico. Y con el fin de tener en cuenta el efecto de la propagación de la señal, se caracteriza el entorno por medio de un conjunto de restricciones de conectividad. La solución ha sido desarrollada

y su validez ha sido demostrada extensamente en aplicaciones reales en entornos subterráneos, en redes malladas y aplicaciones roboticas.

Abstract

One of the consequences of the rapid extension and increasing flexibility of wireless networks in recent years has been the development of mobile ad-hoc networks (MANETs), able to offer services for specific tasks on mobile networks. The mobility and dynamic aspects of mobile network topology combined with the intrinsic requirement of shared media access involve a new set of challenges different from those faced by wired networks. In this context, MANETs have captured the attention of the research community.

Ad-hoc networks usually support best-effort traffic, and several proposals have been put forward to provide minimum bandwidth guarantees or to minimize message delay.

There are situations in which guaranteeing message delivery is not sufficient. This is the case of systems that rely on the guaranteed timely delivery of data, for example real-time systems where the loss or the late arrival of a single piece of data can provoke serious issues. Other applications such as video conferencing are becoming more widespread and the traffic involved has quite different requirements, for example the quality of service (QoS). Real-time and QoS requirements add difficulty to the already demanding problem of offering wireless communication among mobile stations belonging to a MANET.

There are, however, applications in which guaranteeing a reliable network by improving the routing of messages may also be insufficient. This is the case of specific applications in underground areas, where the knowledge of the propagation evolution of the signal between the different nodes can be useful to improve the QoS and to maintain connectivity at all times.

Despite the wide range of proposals in the literature, many of these have several limitations such as the mere use of simulated protocols, isolated proposal from integrated systems or ignoring the effects of environments which are unconventional.

This PhD thesis offers a complete study of a real-time wireless framework using the RT-WMP protocol adapted to the environment and able to manage multimedia flows at the same time. The proposed QoS extension takes advantage of the bandwidth left free by the RT-WMP when it is not working in the worst-case situation. In order to take into account the effect of the signal propagation, the environment has been characterized by a set of connectivity constraints. The solution has been developed and extensively tested in real applications in underground environments involving mesh networks and robotics.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

A Mobile Ad-Hoc Network (MANET) is defined as a collection of self-organized mobile nodes that communicate with each other over radio channels. The advantages offered by MANET include the absence of an infrastructure, independence from a central network or a base station, scalability, low-cost and mobility. These factors have contributed to its increasingly frequent use.

However, ad-hoc network research continues to face the problem of maintaining multi-hop routes despite the challenges posed by mobility, signal interferences, multiple access channels, fading effects, limited bandwidth and power constraints.

These aspects have a noticeable impact on applications that involve distributed Real-Time systems. In these systems, correctness of the task execution is normally expressed as a set of timing constraints that the system has to meet at run-time. It is essential that the communications system, as part of the whole real-time system, offers timing and bounded end-to-end delivery delay guarantees between peers. In recent years, research has been aimed at supplying new wireless communication solutions in order to cope with nontrivial task of providing a set of characteristics, such as time guarantees, deterministic access to the network, and multi-hop, that are not offered by the protocols used in house or in commercial applications.

In certain application fields like rescue or surveillance operations, the possibility of establishing some kind of multimedia communication is useful for obtaining information about both the environment and the people involved. These applications require Quality of Service (QoS) support that adds new requirements and further difficulties to the already demanding problem of offering wireless communication among mobile stations belonging to a Real-Time MANET.

This PhD thesis deals with these issues through a complete study of the Real Time Wireless Multihop Protocol (RT-WMP) [Tardioli 07]. Developed at the University of Zaragoza, the RT-WMP was conceived to connect nodes inside a MANET whose communication requires real-time capabilities. This work focuses on a thorough evaluation and analysis of the protocol and proposes a mechanism to add QoS capabilities. Furthermore, we present a study of the possibility of applying the protocol in confined areas. Finally, in order to validate the study in an actual

MANET, a set of field applications and the related results are presented.

The following sections set out some considerations about communications issues in real-time systems, the challenges of wireless communications and the inadequacy of the 802.11 protocol for transporting time-sensitive data.

1.1 Real-Time communications considerations

Real-time systems are defined as those systems in which the correctness of the system depends not only on the logical result of computation, but also on the time at which the results are produced [Ramamritham 94]. This means there is a set of timing constraints that the system has to meet at run-time.

Mainly due to the geographical distribution, the need to increase fault-tolerance or simply the nature of the application, real-time systems can be constituted by several processing units forming a distributed real-time system. To make a set of systems appear to users as a single coherent system [Tanenbaum 06], distributed systems involve the nontrivial task of maintaining the real-time characteristics of the system as a whole. Otherwise, due to unpredictable communication delays, different nodes may learn of different events at different points in time, causing an incorrect global performance.

As part of the real-time system, the communication network has to effectively cope with timing issues. Unfortunately, most common communication protocols have generally been designed to offer high average bandwidth without taking into account these timing considerations.

1.2 Real-Time wired Communication Protocols

Thanks to its low cost and widespread availability, IEEE 802.3 [Eth 05], popularly called Ethernet, is to date the most widely used wired network architecture. Nodes access the network using the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) technique. Unfortunately, Ethernet resolves collisions using the non-deterministic Binary Exponential Back-Off (BEB) algorithm, while the first requirement for a network to be called real-time is determinism.

In recent decades, several real-time communication protocols have been proposed in order to overcome the Ethernet limitations.

Industrial and professional fields have been the pioneers of the use of the Real-Time communication protocol. Some examples are the Process Field Bus (PROFIBUS) [PBUS 96], the Controller Area Network (CAN) bus [ISO 93], or the Factory Instrumentation Protocol (FIP) [FIP 90]. However they generally require special and dedicated hardware that is not always available in other fields of application.

Some proposals modify the native behavior of the IEEE 802.3 CSMA/CD protocol to avoid collisions [Molle 85] or to sort them in a deterministic manner

[Malcolm 95], [Le Lann 93], [Sobrinho 98].

Another type of solution is the Token-passing paradigm. This makes the access control deterministic allowing a single token owner node to access at once. The idea of token passing, first proposed by [Grow 82], is used in the IEEE 802.4 (Token-bus network) [Damian 00], IEEE 802.5 (Token-ring network) [IEEE 97], and the Fiber Distributed Data Interface (FDDI) [FDD 98] standards, and in the Timed-Token Protocol (TTP) [Malcolm 94], the Real-Time Ethernet Protocol (RETHER) [Venkatramani 94] and the RT-EP protocol [Martínez 03]

In the TDMA scheme, used in the MARZ [Schwarz 02], TTP/C [Kopetz 89] and FlexRay [Pop 06] protocols, each node transmits one after the other, each using its own time slot.

However, there are applications where wiring is a major limitation. This is the case of mobile systems with real-time requirements.

1.3 Real-Time Wireless Communication

The widespread use of wireless networks has been accompanied by a transfer of solutions for wired networks to the wireless medium. However, on the one hand, wireless networks are generally less reliable than wired ones, the probability of errors being much higher. This is due to the possibility of interference, reflections or simply to the distance between peers. Moreover, the fact that nodes are not able to listen to the channel while transmitting aggravates the problem of collision detection and resolution. The vast majority of wireless protocols rely on random backoff mechanisms that introduces a high degree of unpredictability into the Medium Access Control (MAC) layer.

Challenges

Wireless channel Contention The use of a common channel for nodes to communicate among themselves in a MANET introduces the problems of interference and channel contention. These can be avoided in various ways in a peer-to-peer communications network.

One way is to use a system based on th Time Division Multiple Access (TDMA), where each node may transmit at a predefined time, attempting a global clock synchronization. This is difficult to achieve due to the lack of a central controller, the node mobility and the overhead involved.

Another way is to use a different frequency band or spreading code as in Code Division Multiple Access (CDMA) for each node. This requires a mechanism that provides a distributed channel selection as well as channel information dissemination.

An easier way is using a Token passing scheme in order to arbitrate the contention channel. The network generates a single token that permits only the node currently holding it to transmit data.

Indeed, most MANETs are based on the currently most popular wireless ad hoc networking technology 802.11x [IEEE 07]. The 802.11 MAC layer defines two mechanisms to coordinate the access to the medium: the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF).

The DCF scheme employs a Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism, similar to the collision detection CSMA/CD used in wired Ethernet networks. Stations compete to gain the right to access the medium following a non-deterministic inter-frame-delay prioritisation.

Because it is not possible to detect a collision in wireless networks, a collision is identified by means of the absence of the corresponding acknowledgement. So in practice, the CSMA/CA only tries to prevent collisions.

With PCF, a point coordinator within the access point arbitrates which stations can transmit during any given period of time. The point coordinator polls the stations one at a time and if one station has some packet to transmit, it is authorized. During this time no other station can send anything. The point coordinator will then poll the next station and continues down the polling list. Thus, PCF is a contention-free protocol and enables stations to transmit data frames synchronously. However, channel access in PCF mode has the disadvantage of being centralized and seems to be implemented only in very few hardware devices.

Hidden and Exposed node problems The well-understood hidden node and exposed node problems are an additional consequence of channel contention. Hidden node is the situation in which two independent emitters simultaneously send a frame to the same receiver. Exposed node is verified when two transmitters in the range of each other, try to send packets to two receivers that are out of range of each other. This may prevent sending packets.

The Hidden and Exposed node effects are even more pronounced when we consider that nodes may interfere with transmissions outside their transmission range, since receivers are able to detect a signal at a much greater distance than that at which they can decode its information.

Lack of centralized control One of main characteristics of a MANET is the absence of centralized control. It may be set up without planning and its members can change dynamically. As such, communications protocols which utilize only locally available state and operate in a completely distributed manner are preferred [Hanzo-II 07]. However, this generally increases an algorithm's overhead and complexity, as network state information must be disseminated in an efficient way.

Node mobility Node mobility means that any MANET entity may move completely randomly and independently. So mobility entails that topology information has a limited lifetime and must be updated frequently to allow data packets to be routed to their destinations.

This characteristic could invalidate any link stability guarantees or hard packet delivery ratios [Qin 06]. So, as a general assumption for any routing protocol able to function properly, the topology changing rate must be less than or equal to the rate of state information propagation. Otherwise, routing will be inefficient or even fail completely because the information will always be stale.

Limited device resources Although mobile devices are becoming more and more powerful and capable, it still holds true that they generally have less computational power, less memory, and a limited power supply compared to computers typically employed in wired networks. Limited resources have a major impact on the provision of QoS assurances, since low memory capacity limits the amount of QoS state that can be stored, necessitating more frequent updates which incurs greater overhead. Additionally, Real-Time and QoS routing generally implies a greater overhead than best-effort routing due to the extra information being disseminated. These factors may place an undue burden on a less-powerful processor and limit battery power supply.

Signal Propagation and Environment Several studies have been made about signal propagation taking into account antenna polarization, operating frequency and characteristics of the environment. Propagation models are different depending on whether the wave is propagating in free space, indoors, in urban environments or in confined environments. Nevertheless, many valuable studies in the area of MANET have been carried out by computer simulations or experiments. Most of them do not consider the signal propagation or the propagation environment at all. However, in order to make optimal use of a MANET, it is desirable to have some knowledge of both characteristics because a solution for a certain environment may not work effectively in a different environment. This is especially true in applications carried out in confined environments such as tunnels or mines where success of the operation could depend on providing communications capability according to the environmental settings.

Given all these issues, the scientific community is divided on the possibility of supporting real-time traffic via wireless communication. This is understandable considering that a single missed deadline can provoke a total system failure. However, no system is exempt from errors or problems. Even a very robust system can suffer from electrical or mechanical problems that can jeopardize its correct behavior. Real-time protocols rely on the fact that the probability of errors is below a certain reasonable threshold. Ethernet and real-time ethernet, for example, manage Bit Error Ratios (BER) of about 10^{-10}. This means that a 100 Mbps saturated network suffers from an error each 100 seconds or for each 1.215 GB transferred.

Thus, a common real-time system must be able to manage at least such a level of probability of error without ending in total failure. Obviously it is impossible to obtain such BERs in wireless communications (they are at least a couple of orders of magnitude apart), at least with the current technology. However, if a particular system can tolerate a higher probability of error then it is possible, in our opinion, to speak at least of *firm* real-time wireless communication.

In cooperative robotics applications this is sometimes enough. Due to the autonomy of the nodes, infrequent deadline misses could be tolerable even if they degrade the quality of service of the system.

In these applications robots, in fact, need to collaborate to achieve a common goal. Generally, sensors on the robots produce periodic updates that must be transmitted to other members of the team respecting time constraints to enable such collaboration to take place [Stankovic 04]. The strictness of the timing requirements depends on the specific application or system, but the loss of a single or multiple deadlines is not necessarily a great problem.

Just to give an example, consider a team of mobile robots with the task of cooperatively building a map, such as in [Urcola 09]. The slave robots share their laser-range readings with the leader of the team to build a common and more complete view of the environment. Knowing the maximum end-to-end delay is critical to correctly position the readings in time and thus in the corresponding period of the control algorithm. The loss of a single reading is not critical since the leader can rely on the previous observations and avoid the updating of the map in a single control loop iteration without degrading the quality of the map very much.

The example above also highlights that such real-time capability must be guaranteed not only in static but also in dynamic scenarios when considering mobile robotics applications. In other words, it is necessary to provide for *mobility* and *multi-hop* in order not to restrict the freedom of the team members. It is also necessary to provide support for message priority allowing for both task planning of the whole system and for carrying different flows of messages (consider for example control and supervision flows).

1.4 Quality of Service considerations

In certain fields of application, the possibility of managing another type of traffic together with the real-time traffic could be useful. For example, some type of multimedia communication could be established while the real-time capabilities of the network are still guaranteed. Although multimedia flow has strict time requirements, it can not be treated as a real-time flow. It might therefore be a good idea to take into account these flows considering another constraints.

Quality of service (QoS) is defined as the performance level of a service offered by the network to the user. The goal of QoS provisioning is to accomplish better delivery of the information carried by the network and better utilization of the network resources [Reddy 06].

In the literature, the QoS challenge in ad hoc networks has been faced by trying to guarantee limited end-to-end delay and minimum bandwidth for specific flows. These requirements arise with delay sensitive applications such as video and audio streams. In a wireless environment, however, it is difficult to guarantee QoS given the unpredictability of the medium. Moreover, it is a major challenge to distinguish between frame losses due to collisions and congestions, or erroneous receptions because of a high bit error rate. The distributed scheme and the dependency on other stations to forward data frames in multihop communications further aggravate the problem.

In order to specify QoS requirements, application protocols have to consider a set of metrics to define constraints. An application may typically request a particular QoS by specifying its requirements in terms of one or more of the metrics presented in the following list. These metrics, especially those measured at lower layers, are not of direct interest to the application layer. However, they all directly or indirectly affect the QoS of a data session.

Network Layer Metrics

Throughput It is the desired data throughput for the application. Most of Adhoc network routing technique using this metric/constraint.

Delay The End-to-End Delay (E2E) represents the delay from source to destination experienced by a packet to be transmitted across a network. Multimedia traffic is delay-sensitive and live audio-visual communication requires that the end-to-end delay be less than a certain value. Thus, audio/video applications usually define the maximum admitted E2E: the global value has to stay of less than some levels to ensure good interactivity between users [Chen 99].

Jitter Jitter is the measure of the variability over time of the latency across a network. In other words, it represents the variation in the delay of received packets in a flow, measured by comparing the interval when the packets were sent to the interval at which they were received. Jitter turns out to be an important QoS parameter in audio stream, which is strongly related to synchronization and packet buffering along the network [Wang 05].

Packet Delivery Ratio (PDR) The acceptable percentage of total packets delivered at the final destination node, which are sent by the transport or higher layer agent from the source node [Abdrabou 06]. PDR is one of the most popularly used metric for assessing a link's quality and it could be used as a main determinant for rate selection decisions or routing.

MOS Previous metrics can be measured quantitatively, but multimedia quality can require human interpretation even though a quality estimate can be made by automatic test systems. Mean Opinion Score (MOS) [ITU-T 99] provides a numerical indication of the perceived quality of received media after compression and/or transmission of multimedia (audio, voice telephony, or video). The MOS is expressed as a single number in the range 1 (lowest perceived quality) to 5 (highest perceived quality) and is generated by averaging the results of a set of standard and subjective tests.

Link and Physical Layer Metrics

SINR Signal to Interference plus Noise Ratio (SINR) represents the extent to which the power of the received signal exceeds the sum of noise plus interference at the receiver. Recent studies have considered SINR to be the most appropriate metric for quantifying the quality of a link. However, the instantaneous SINR value cannot be easily computed because commercial wireless cards do not report it during the reception of a packet [Vlavianos 08].

BER Bit Error Rate (BER) represents the ratio of bits with errors to the total number of bits that have been received over a given time period. In others words, BER measures the probability that a bit gets flipped, i.e. it is received in error. This is one of the most important measures of digital communication performance [Goldsmith 05]. However, measuring the BER is a non-trivial task and, in practice, no commercial card implements the BER measure.

RSSI Receive Signal Strength Indication (RSSI) is a dimensionless quantity which represents the signal strength observed by the receiver during packet reception. Although RSSI is not considered as the best stand-alone metric because it does not capture the amount of destructive interference on links, it is easy to measure. Commercial cards provide the RSSI while receiving packets. Under certain conditions, this can be considered a promising metric [Srinivasan 06].

Link Stability Variations in the received signal strength and the asymmetrical behavior of links may provide a hint of the movement pattern of the connection peers and thus allow an estimation of a probable connection loss [Wang 06]. However, received signal strength is largely dependent on actual radio conditions. Due to fading effects these measurements are subject to large fluctuations.

1.5 802.11 for Real Time Wireless applications?

As explained earlier, real-time communication is necessary in applications where shared information is time-sensitive, as for example applications involving robot teams.

Commercial wireless devices are based on IEEE 802.11 which has become the standard for wireless networking thanks to its wide diffusion. Its standardisation and the low price of the devices have been the key factors for its wide acceptance. However, the 802.11 protocol does not offer any facility to support the exchange of time-sensitive data in MANETs because it lacks deterministic behavior. It uses a random backoff mechanism for medium access and collision resolution. This makes the use of this solution impossible in real-time networks where all the phases of the communication are required to be time-bounded. Moreover, the protocol is not able to manage (natively) multi-hop peer-to-peer communication, and mobility is restricted to the collision domain shared by the members of the network.

Random backoff

Neither the backoff nor the RTS/CTS mechanisms eliminate the possibility of collision. In fact, two or more stations can choose the same backoff period and begin transmission at precisely the same moment. Moreover, the presence of *random* factors in transmission deferral implies timing indeterminism in information exchange. This factor can lead to situations such as the false blocking problem [Ray 03] that can completely jeopardize the operation of a wireless network. This precludes the use of the plain 802.11 protocol for real-time communication and demonstrates the need for a deterministic alternative.

Multi-hop

The 802.11 was intended primarily to grant wireless access to the internet by means of access points connected to the network infrastructure. In this configuration, all the stations must be able to communicate directly with the access point that distributes the frame acting as a bridge. The ad-hoc mode allows, instead, peer-to-peer communication but, as stated earlier, does not support multi-hop. Stations in their respective communication range can communicate with each other but 802.11 does not provide any routing algorithm to propagate information among nodes which are far apart.

This feature has to be implemented by means of upper layer routing protocols such as AODV [Perkins 03], DSDV [Perkins 94], etc. However, regardless of the overhead introduced by the routing protocol used, end-to-end bandwidth is highly dependent on network topology and the number of nodes in the network. In fact, according to [Sobrinho 99], a transmission can cause interference in a range larger than the communication range (almost twice the latter). Nodes within the *carrier sensing range* of a transmitting node can sense the carrier of the sender even if they can not hear the frame, and thus delay its transmission. According to our research, in relatively small wireless networks there can be situations where each node can only communicate with its predecessor and its successor, and carrier sensing does

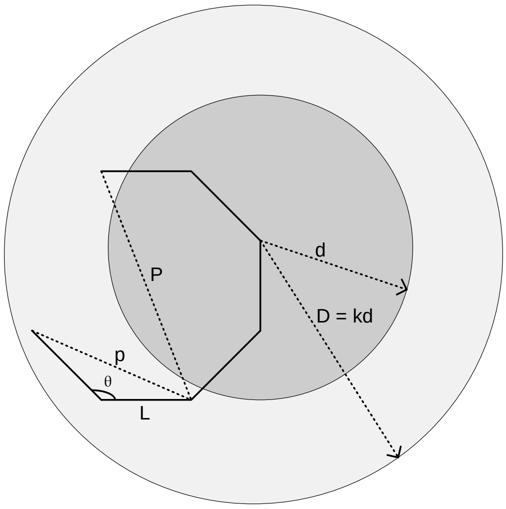


Figure 1.1: Visual representation of a zone in which neither spatial reuse nor broadcast dissemination is possible.

not allow spatial reuse (i.e. only *one* node can transmit at a time). In short, sometimes neither spatial reuse nor broadcast dissemination is possible.

Let us show an example: consider d to be the communication range of two nodes and $D = kd$ the corresponding *carrier sensing* range (defined as the distance within which a node will detect an existing transmission with high probability by using the physical carrier sensing mechanism [Yang 05]), proportional to d by means of the constant k. Nodes within carrier sensing range of each other will not transmit at the same time since they consider the channel to be busy.

Carrier sensing range is usually considered to be *at least* 2.2 times the communication range. The ns-2 simulator [NS2 11], for example, fixes by default the communication range at 250 m and the carrier sensing range at 550 m. Experimental results give even worse scenarios, especially for high rates [Anastasi 04]. In the light of this, if we impose the conditions (consider fig. 1.1):

$$\begin{cases} L \leq d \\ P < D = kd \\ p > d \end{cases} \tag{1.1}$$

L being the distance between adjacent nodes, p being the minimum distance between each pair of non-adjacent nodes and P the maximum distance between each pair of nodes, we can find networks in which all the nodes are in the carrier sensing range of each other *and* each node can communicate *only* with its adjacent neighbors (single transmitter area, STA). Considering $k = 2.2$, for example, a network with nodes in twelve of the thirteen vertices of a regular tridecagon with edges $L = 0.52d$ would satisfy these conditions. Moreover, the greater the value of

k, the larger the STA.

Since during the free movement of the nodes a topological configuration like the one described in the previous example could be achieved, this must be taken into account when designing a routing algorithm, especially a real-time one.

In such a situation, the end-to-end bandwidth depends on the number of hops separating the sender from the receiver. The *worst-case situation* occurs when the source and the destination are $n-1$ hops away, n being the number of nodes in the network. In this case the available bandwidth of the 802.11 protocol can be expressed as:

$$BW_{end\_to\_end} = \frac{BW_{channel}}{(n-1)} \tag{1.2}$$

In [Ng 07], through simulation and experimental results, the authors show that in a four node chain 11 Mbps network, *end-to-end* throughput can reach values close to 2 Mbps, whereas for a six node chain the result is approximately 1.2 Mbps, values that match the calculus above.

In short, even though use of the 802.11 protocol is very widespread thanks to its notable characteristics such as its relatively high bandwidth, good communication range and the low cost of the devices, it does not constitute an option for real-time communication in robotics due to the lack of multi-hop support and the indeterminism that affects the MAC layer.

1.6 Goals and contributions

As has been seen, developing a real-time MANETs and its application involves a set of challenges whose solution remains open.

This PhD thesis addresses a set of problems related with the use of a real-time ad-hoc network applied in actual applications. The RT-WMP protocol, developed at the University of Zaragoza, is used in order to provide an effective network amongst nodes. At the time of writing, this protocol seems to be one of the few solutions that allows real-time characteristics to be guaranteed for wireless networks that has actually been implemented, to the best of our knowledge. No protocol with all of these features has appeared in the literature.

Starting from the protocol definition, we make an in-depth evaluation and analysis of the protocol. The first contribution of this work is to characterize the protocol in terms of both theory and practice. This results a practical evaluation of a type which can scarcely be found in the literature given that most network evaluations are carried out in simulated environments.

The second contribution involves meeting the requirements for multimedia flow support in addition to real-time support. This is possible offering QoS, together with real-time support, by means of developing an extension to the protocol. The extension capability offers the possibility of establishing voice and video links among mobile nodes without altering the worst-case characteristics of the RT-WMP, taking advantage of the fact that the basic protocol works in worst-case situations in very few cases.

The development of a real-time wireless protocol with QoS capability is of great interest in applications such as rescues in disaster scenarios involving humans. In this context, confined areas are of particular interest from the point of view of the difficulties of providing an efficient communication service. This stems from the fact that in environments such as tunnels or mines, common radio systems provide an ineffectual or at best a very limited communications capability.

A third contribution of this thesis is towards to perform a study about some signal propagation aspects and a set of real measurement in this kind environments. This environment characterization is in view of perform real underground communication applications using MANETs.

A third contribution of this thesis is the study of certain aspects of signal propagation and the provision of a set of real measurements in confined environments. This environment characterization is achieved through the application of real underground communication systems using MANETs.

In fact, the latter contribution is the implementation of a set of field applications in confined settings where the protocol performance and effectiveness are demonstrated from the points of view of real-time characteristics, QoS capabilities and specialization to the specific environment.

1.7 Structure of the Thesis

This thesis is organized as follows. In the next chapter the basic protocol RT-WMP and its characteristics are presented.

Chapter 3 is dedicated to a thorough evaluation of the protocol, taking into account theoretical timing features, real measurements, mobility capabilities and a comparison with a general purpose protocol. The chapter also presents an analysis of the protocol considering the planning of tasks, compliance of timing requirements and overload.

Chapter 4 details the QoS extension of the protocol that introduces a technique to allow the delivery of multimedia messages with few overheads and the management of variable priority messages without compromising the RT-WMP worst-case end-to-end delivery delay.

Chapter 5 examines the possibility of applying the protocol in confined areas. A study is carried out and a set of real measurements obtained relating to the propagation of the wireless signal and the metrics used for the MANETs. The work is focused on so-called fading environments, providing an analysis of the signal propagation in order obtain the general characteristic parameters of this kind of environment.

Chapters 6 describes three real test scenarios covering aspects that of ad-hoc network and robotics applications. The first presents the RT-WMP that, in this case, is used to manage multimedia communication between a pair of mobile nodes located in the confined environment of a linear tunnel linking Spain with France. The second test scenario shows an experimental application involving real robots and human operators in a system which integrates several research issues aimed at achieving a real exploration in a tunnel. Real-time, QoS support and guaranteeing connectivity at all times were the communication targets of this framework. The final application consists of a planning technique used to deploy a team of robots in fading environments. The technique, via real time signal measurements, is based on the use of characteristic parameters of these environments. The system as a whole is evaluated by means of simulation and in a real scenario.

Finally, the last chapter sets out the conclusions of this thesis and proposals for future work.

Chapter 2

RT-WMP Definition

The RT-WMP protocol was conceived to connect small teams of robots whose communication requires real-time capabilities. The idea was to develop a real-time protocol to guarantee the delivery of time sensitive data within bounded delays over a multi-hop path. The protocol is capable of managing message priority and mobility both outdoors and in confined areas such as buildings, tunnels, mines or hostile environments in general.

At the time, no protocol with all of these features had appeared in the literature or had been implemented, to the best of our knowledge. This is a novel protocol for MANETs that supports *real-time* traffic. In fact, in RT-WMP end-to-end message delay has a *bounded and known duration* and it also manages global static message *priorities*. Besides, RT-WMP supports *multi-hop* communications to increase network coverage. The protocol has been designed to connect a relatively small group of mobile nodes (up to 32 units maximum). It is based on a token passing scheme and is completely decentralized. Any topology of the network will suffice. The protocol is designed to manage rapid topology changes through the sharing of a new type of adjacency matrix containing link quality amongst nodes. RT-WMP has a built-in efficient error management mechanism that can recover from certain types of errors without jeopardizing real-time behavior. A technique for reincorporating lost nodes is also proposed. The RT-WMP can run over 802.11 *commercial hardware* without modifications and eliminates the protocol's own indeterminism at the MAC layer.

The firt version of the protocol was presented at The Fourth IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS) at the end of 2007 [Tardioli 07]. The protocol is currently *implemented* on the Linux and MaRTE OS [Rivas 01] platforms. Its functionality has been extensively tested and it is used to support communication in several real applications, as we will show in the following chapters of this thesis.

2.1 Related Work

The literature on how to support real-time communication in wireless environments is not very vast. However, several proposals have been put forward in the last few years.

In early 1997, Lin and Gerla [Lin 97] proposed a solution for the flows of multimedia data that takes advantage of a TDMA technique in which nodes can reserve time slots over the path that connects them with their destination nodes. An interesting aspect of the solution is the so called *QoS routing*, in which each node saves information about the network topology with respect to the bandwidth. Periodically, nodes send this information to the other nodes. The drawback of the use of TDMA schemes is the difficult synchronization between the local clocks of the nodes.

In [Ye 01] and [Pradhan 98], one or more Access Points coordinate the access to the medium. In general, these solutions are improvements on the 802.11-native Point Coordination Function (PCF) protocol, which is infrastructure-based and presents the same restrictions in terms of mobility.

In other solutions, a node that needs to transmit occupies the medium with energy pulses [Sobrinho 96, Sheu 04], the duration of which is proportional to the priority of the node. If nodes try to transmit simultaneously, the station with the highest priority will be the only one to find the medium idle when it ceases to transmit. In this way, the station with the highest priority knows that it has won contention for the channel. In general, these solutions do not address the problem of the hidden terminal, that remains unresolved [Kosek-Szott 12], and require hardware modification.

In the WTRP protocol [Lee 02], Lee et al. proposed a token-ring network based on the ideas of the 802.4 token bus protocol [Damian 00]. When a node receives the token, it can transmit for a fixed time. At the end of the transmission, the node passes the token to its successor. Network activity after the token is passed on is interpreted by the sender as an implicit acknowledgment. If the acknowledgment fails, the node tries to reconstruct the ring excluding as few nodes as possible. However, in some cases the need to close the ring can lead to the exclusion of many nodes. Besides, multi-hop communication is not supported, since a node can only communicate with its neighbors.

Donatiello and Furini [Donatiello 03] propose a similar token-passing solution, in which nodes are also organized in a ring. The token always travels in the same direction and messages travel through the nodes belonging to the ring to reach the destination. The need to keep the ring connected introduces many limitations in terms of mobility, since multi-hop communication is possible only by maintaining the ring topology. The solution proposes an interesting spatial-reuse technique based on a Code Division Multiple Access (CDMA) modulation. Unfortunately, CDMA devices are not common consumer products like 802.11 cards, even though this modulation is widely used in mobile phones.

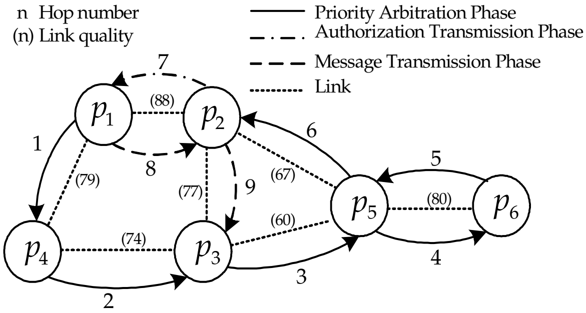
Al-Karaki and Chang [Al-Karaki 04] proposed the EPCF protocol, which is a 802.11-native PCF protocol extension. The enhancement of the protocol is in the polling phase because EPCF incorporates priorities. In the case of multi-hop network environments, some nodes play the role of Virtual Access Point and the net is organized hierarchically. In [Alonso-Zarate 12], with a similar approach, authors propose a Distributed Point Coordination Function (DPCF) as a combination of the DCF and the PCF of the IEEE 802.11 in order to improve the performance of wireless ad-hoc networks under heavy traffic load conditions. However, these papers do not clearly explain either the steps required to set-up a multi-hop network or the related temporization. Moreover, at the moment there is no existing implementation of these protocol.

In [Facchinetti 05], Buttazzo et al. proposed another interesting solution based on a time division scheme. This paper proposes the use of implicit EDF to provide real-time guarantees. Collisions are avoided by replicating and executing the EDF scheduler in parallel in all nodes. Communication amongst nodes is organized in consecutive slots, referred to as system ticks, the duration of which is constant. *Connectivity tracking* is carried out through the exchange of each node's adjacency matrix, in order to make all the matrices converge toward the unique and correct view of the entire network. However, this solution does not support user-message multi-hop.

In late 2005, though, the IEEE approved the 802.11e [IEEE 05] specification. This standard is a set of technologies for prioritizing traffic, which adds QoS capability to the 802.11 legacy protocol. The 802.11e introduces a new Hybrid Coordination Function (HCF) that replaces the legacy of DCF and PCF. Within the HCF, there are two access mechanisms, the Enhanced Distributed Channel Access (EDCA) and the HCF Controlled Channel Access (HCCA). While HCCA is a centralized access method, ECDA can be used in ad-hoc networks. EDCA contention access includes priorities by introducing eight priority queues in which messages contend for the right to transmit. However, even if contention windows and backoff times are adjusted to favor messages with the highest priority, collisions can still occur and the resolution mechanism is based on the calculation of a *random* backoff time that is incompatible with real-time planning, just as in the 802.11 legacy protocol. Besides, the legacy 802.11e standard does not offer multi-hop routing and additional routing protocols have to be used.

An interesting extension to the 802.11e that includes multi-hop traffic support is presented in [Reddy 07]. In this solution packets are prioritized using a combination of the laxity of the packet and the number of hops to the destination node to give higher priority to the packets that have to traverse many hops. However, this solution involves the modification of the 802.11e protocol to store additional information in its queues. Moreover, like the 802.11e legacy protocol, it has been conceived to deal with multimedia traffic that has slightly different requisites from the real-time one.

In short, even if solutions for support of real-time traffic over ad-hoc wireless



Link Quality Matrix

	p_1	p_2	p_3	p_4	p_5	p_6
p_1	-	88	0	79	0	0
p_2	88	-	77	0	67	0
p_3	0	77	-	74	60	0
p_4	79	0	74	-	0	0
p_5	0	67	60	0	-	80
p_6	0	0	0	0	80	-

Figure 2.1: A hypothetical situation described by the network graph and the corresponding LQM. The hops sequence of the protocol is also shown.

network exist, there are no solutions that deal globally and completely with real-time and mobile multi-hop requisites. Instead, in some protocols priorities are only supported at node level and not at message level. Besides, very few of the protocols set forth have actually been implemented.

2.2 Overview

The system architecture considered consists of a S set of n mobile nodes $S = \{p_0, ..., p_{n-1}\}$ which can communicate over a wireless link.

All the nodes use a single *shared* radio channel to exchange messages. We call the subset of nodes that can hear the transmission of node p_i *neighbors* of node p_i. Each node has a transmission and a reception priority queue. Each message exchanged between nodes is identified by a priority level in the $[0, 127]$ range, where 127 is the highest priority value. Messages with the same priority are stored in FIFO order. When an application needs to transmit a message to another node, it pushes it into the transmission queue. The RT-WMP process pops the message from that queue and transmits it through the network to the destination node. The latter pushes the message into the reception queue and the destination application can finally pop the message from that queue.

The protocol works in three phases (see figure 2.1): *Priority Arbitration Phase (PAP)*, *Authorization Transmission Phase (ATP)* and *Message Transmission Phase (MTP)*.

During the PAP, nodes reach a consensus over which of them holds the Most Priority Message (MPM) in the network at that moment. Subsequently, in the ATP, an authorization to transmit is sent to the node which holds the highest priority message. Finally, in the MTP, this node sends the message to the destination node.

To reach a consensus over which node holds the highest priority message, in the PAP a token travels through all of the nodes. The token holds information on the header (drop)

res	serial	type	src	dst
1	1	1	1	1

token

max_pri	max_pri_id	age	lack	nstat	LQM
1	1	2	1	n	n^2 - n

authorization

aut_src	aut_dst	nyr
1	1	n (bit)

message

msg_src	msg_dst	nyr	priority	len	message
1	1	n (bit)	1	2	0..M T U

Figure 2.2: Frames of the protocol. Field size is expressed in bytes.

priority level of the MPM in the network and its owner amongst the set of nodes already reached by the token.

The node which initiates the PAP states that the highest priority message in its own queue is the MPM in the whole network and stores this information in the token. Then it sends the token to another node, which checks the messages in its own queue. If the node verifies that it holds a message with a higher priority than the one carried by the token, it modifies the token data and continues the phase. The last node to receive the token, which knows the identity of the MPM holder, closes the PAP and initiates the ATP.

In this phase, the node calculates a path to the MPM holder using the topology information shared amongst the members of the network (the Link Quality Matrix, see below) and sends an authorization message to the first node in the path. The latter will route the message to the second node in the path and so on, until the authorization reaches the MPM holder. This is when the MTP begins. The development of this phase is quite similar to the preceding one. The node that has received the authorization calculates the path to reach the destination, and sends the message to the first node of the path. The message follows the path and eventually reaches its destination. Phases repeat one after another i.e., when the MTP finishes, the node destination of the message initiates a new PAP an so on. When none of the nodes have a message to transmit, the authorization and message transmission phase are omitted and priority arbitration phases repeat continuously. The succession of events that can bring to the delivery of a message (a succession of PAP, ATP and MTP or PAP and MTP or even a single PAP if there are not messages to be send) are called *loop*. This can be seen also as the time lapse between two consecutive PAPs.

2.3 Frames Definition

In figure 2.2 frames exchanged amongst nodes are presented. The frames have a common header and an extra part that is different for each frame type. In the header, the first byte (*res*) is reserved for communication between the network interface card (NIC) driver and the RT-WMP process. The *serial* field contains the serial number of the frame. This field is used in the error recovery mechanism (see sec. 2.7) together with the *retries* field (1 byte). The *type* field identifies the type of the frame (*token, authorization, message* or *drop*). The *src* and *dst* fields contain information about the source and the destination of the frame. In fact, in the RT-WMP, nodes are identified through a natural number between 0 and $n-1$ called the WMP address, n being the fixed number of the nodes in the network. When a node needs to send a frame (of any type), it fills the *src* and *dst* fields of the header with its WMP address and the WMP address of the destination node and broadcasts the frame. Since the radio channel is shared, all the neighbors of the sender hear the frame but only the destination processes it. The *token* frame adds the *max_pri* and *max_pri_id* fields that carry the MPM priority level and the MPM holder WMP address. The *age* field is used to keep track of the oldest message amongst messages with the same priority level. The *lack* field is used for *belated acknowledgement* of the sender (see sec. 2.5.3). The *nstat* field is an array of n bytes. The value *nstat[i]* represents the status of the p_i node that can be *unreached, reached, lost* and *searched*. Finally, the *LQM* field contains the LQM. The *authorization* frame adds the *aut_dst* and *aut_src* fields that carry the address of the destination node and of the source of the authorization to the common header and the *nyr* variable length field (1 bit for each one of the nodes in the network), also present in the message frame that is used to avoid infinite loops in authorization and message delivery (see sec. 2.7.1 for details). The *message* frame type holds the *msg_src* and *msg_dst* field that contain the WMP address of the source and of the message destination. The *priority* and *len* fields hold the priority and the length of the data carried by the frame as well. The field *data* contains the payload of the frame, which can have a length between 0 and *MTU* bytes. Finally, the *drop* frame is a simple header and is identified through the *type* field.

2.4 The Link Quality Matrix

To describe the topology of the network, RT-WMP defines an extension of the network connectivity graph (as defined in [Facchinetti 05]) adding nonnegative values on the edges of the graph. These values are calculated as functions of the *radio signal* between pairs of nodes and are indicators of *link quality* between them. These values are represented in a matrix called the Link Quality Matrix (LQM), the elements of which $lqm_{ij} \epsilon [0, max\_lq]$ describe link quality between p_i and p_j nodes (see figure 2.1). Each line LQM_k describes the links of the p_k node with its neighbors. Even if the links can be asymmetric (the radio signal received by p_i when p_j transmits can be different from the one received by p_j when $p_i$transmits), generally the differences are very small. In any case, at the moment of computing the path using these values, the protocol chooses the minimum value $lqm_{ij}(min)$ between the two correspondent in the matrix ($lqm_{ij}(min) = min(lqm_{ij}, lqm_{ji})$. Consequently, at any moment the protocol is working with a symmetrical LQM. The nodes use this matrix to select which node to pass the token to and to take decisions on the best path to route a message from a source to a destination. All the nodes have a local copy of the LQM that is updated each time a frame is received. Besides, every node is responsible for updating its line of the LQM (both in the local copy and the shared copy) to inform the other nodes about local topology changes.

2.5 Phases of the Protocol

In the following sections, we offer a detailed description of the three phases of the protocol. Let us suppose that all the nodes know the network topology (i.e. all the nodes have the same LQM) and that the network is connected. In these sections, we also presuppose that the nodes stay put and that communication is error free. These limitations will be treated in the sections 2.6 and 2.7 respectively.

2.5.1 Priority Arbitration Phase

The first phase is the priority arbitration phase. When a p_k node initiates the PAP, it creates a new token, copies its local LQM in the relevant field of the token and sets the $nstat[i]$ to *unreached* $\forall\ i \in [0, n-1]\ :\ i \neq k$. The value $nstat[k]$ will be set instead to *reached*. This means that, in the current PAP, none of the nodes have been reached by the token yet, except the p_k node. Afterwards, it checks the priority level of the highest priority message in its transmission queue and sets the *max_pri* and *max_pri_id* fields with this value and its WMP address respectively. The *age* field is filled with the age of the message (i.e. the time that the message has spent in the queue up to that moment) expressed in milliseconds. In this way, the p_k node is stating that it is the MPM holder. Then, it analyzes the LQM to know with which p_{bl} node it shares the best link quality, and sends the token to it. When p_{bl} receives the token, it sets the $nstat[bl]$ to *reached*, updates the *LQM* token field with its local data and saves the matrix locally. It subsequently increases the value of the age field by a quantity equal to the duration of one token-pass hop, in order to update the age of the message that the token refers to. Then it looks for the value of the *max_pri* field of the token and compares it with the priority level of the highest priority message in its queue. If it verifies that it holds a higher priority message, it modifies the *max_pri* and *max_pri_id* fields. If it holds a message with the same priority, however, it checks the *age* field of the token. If the message is older than the one carried by the token, it updates the token as well. Subsequently, it chooses the node with which it shares the best link quality *amongst the set of nodes not yet reached*, and sends the token to it. If a node only listens to its predecessor (i.e. the node that passed the token to it), it can return the token to the predecessor after updating. This means that a node can receive the token several times during the same PAP. In that case it has the right to update the *max_pri* and *max_pri_id* values. This behavior helps reduce the well-known priority inversion problem. The process is repeated until all the nodes have been reached by the token (i.e. $nstat[i] = reached \; \forall \; i$). The last node to receive the token knows the MPM holder's identity (which is contained in the *max_pri_id* field) and is responsible for sending it the authorization. This node ends the PAP and initiates the ATP.

2.5.2 Authorization Transmission Phase

First of all, the node that starts the ATP calculates a path to reach the destination node. To do this, it applies the well known Dijkstra algorithm [Dijkstra 59] to a distance matrix derived from the LQM as described in section 2.6.3. The Dijkstra algorithm returns a path to the destination as a set $P = \{p_{p_1}..p_{p_m}\}$ of nodes. Then the node creates an *authorization* and fills the *aut_dest* and *aut_src* fields with the MPM holder address and its own address respectively, and sends the authorization to the first node of the path. When p_{p_1} receives the authorization, it looks at the *aut_dest* field and if it contains its address, it ends the ATP and initiates the MTP. Otherwise, it calculates the $P' = \{p'_{p_1}..p'_{p_{(m-1)}}\}$ path, where $p'_{p_k} = p_{p_{(k+1)}} \; {}_{k<m}$. In other words, since the calculation is executed over the same LQM, the path calculated will be the same, except that the first hop has already taken place. Since all the nodes have the same topological information, recalculation of the path in each hop allows the saving of the bandwidth needed to propagate it. The node repeats the process just explained, routing the message to the next member of the path, leaving the *aut_dest* field unchanged.

2.5.3 Message Transmission Phase

When the MPM holder receives the authorization to transmit, it takes the highest priority message out from its transmission queue, creates a new *message* frame and places the data in the *data* field. It fills the *msg_src* and *msg_dest* fields with its address and with the destination address and calculates the path to the destination, just like in the ATP. Then it fills the *priority* and *len* fields with the message's priority and data length and sends it to the first node that belongs to the path. When the latter receives the message, it checks the *msg_dest* field. If it contains its address (i.e. if it is the destination) it pushes the message into the receiption queue and starts a new PAP. Otherwise, it repeats the computation of the path and repeats the process just explained, routing the message to the next member of the path and leaving the *msg_dest* field unchanged.

An explicit acknowledgment is not included because it would create too much overhead. However, if the message reaches the destination node, the latter introduces its WMP address in the *lack* field of the new token before initiating the new PAP. During this PAP, the token will reach the sender of the previous message, who can check if the message has been delivered or not by looking at the *lack* field.

2.6 Mobility Management

Topology can change frequently in MANETS. If nodes are moving, the radio signal and therefore link quality amongst them varies and these changes must be rapidly reflected in the global status of the network. Consequently, when a node discovers a change, it has to propagate this information as soon as possible. In RT-WMP this task is carried out by the token in the PAP phases. In fact, topological information travels with it in the LQM and is updated in each hop.

2.6.1 LQM Updating

As explained earlier, each line LQM_k of the LQM describes the links of the p_k node with all the nodes of the network. Nodes can easily obtain information to fill the relevant line of the matrix. In fact, when a node sends a frame of any type, its neighbors - due to the broadcasting nature of the wireless medium - listen to the transmission and read the radio signal from the network layer to update its local LQM. These changes have to be reflected in the shared LQM as soon as possible, to allow the nodes to correctly calculate the paths in the ATP and MTP. Therefore, when a p_k node receives a token, it updates the LQM_k line of the LQM token field, saves the whole matrix locally to use it in the successive ATP and MTP, and then retransmits it. Since the LQM reaches all the nodes frequently, they have accurate and up-to-date information on the network's (link-quality) topology. Consequently, if two nodes are moving away from each other, link quality will gradually fall until it reaches a value close to zero, after which the link is lost. This value is reflected in the LQM, and nodes, whenever possible, will avoid that link to route information when link quality is beneath a certain threshold.

In any case, due to the technique used to update the LQM, the value 0 never would appear, and the last positive value would be maintained until an error were verified (see section 2.7). To avoid this behavior, a timeout on the validity of the values of the local LQM elements called LQM Element Validity Period (LEVP) has been introduced. If the p_k node has a local LQM where $lqm_{kl} > 0$ but does not hear a transmission from node p_l within a certain timeout, then p_k supposes that p_l is not near it yet, and sets that value to 0. In this way, in the successive PAPs other nodes will know that p_k can not communicate with p_l anymore and avoid this link for subsequent paths computation.

The frequency with which each node receives the token and thus update the LQM, depends on the number of nodes, on the maximum message size and on network rate. However, as it is easily to calculate, it hover around few centimeters for common rates and moderate speeds. However, there is an additional method to maintain the LQM up-to-date. When a node sends a token, all of its neighbors receive the frame. While the destination processes the frame and makes the appropriate decision, the other nodes update their local information on link quality with the sender, as explained earlier. Moreover, if the frame received contains a more recent LQM they can use it to update their own.

2.6.2 Maintaining a fresh LQM

These techniques guarantee that LQM reflects the topology of the network well in the most part of the situations. However, there exist a particular configuration in which the quality of the information contained in the LQM can degrade fastly.

Let consider a chain network $p_1..p_n$ in which p_a starts the PAP and p_a is always (or during a long period interval) the owner of the most priority message which destination is, in turn, p_a . The PAP will develop as $p_a \rightarrow p_b \ldots \rightarrow p_n$, then p_n will authorize itself and will send the message to p_a through the chain. In this configuration, the p_n node *never* has the possibility of sending its own view of the network (its LQM) and if it is moving, for example, the other nodes can not know the status of the links. To avoid this behavior a technique to force the execution of a worst-case PAP has been introduced in the protocol. When a node is not able to propagate its LQM during a configurable number of loops, it can request to force a worst-case PAP in which all the node have the opportunity of sending a token frame. In the example above, node p_n can force a worst-case PAP, modifing the token frame when received: it states that node p_b has not been reached in the current PAP and send the token back to p_{n-1} that propagate it back up to p_2 where the $2n-3$-hops PAP ends.

This technique does not alter the real-time behavior of the protocol since, as anticipated, the planner has always to take into account the worst-case duration of each one of the RT-WMP phases.

2.6.3 LQM Elements and Path Calculation

As mentioned earlier, the lqm_{ij} elements of the LQM are functions of the radio signal links between nodes. To calculate them, we use the *Received Signal Strength Indicator* (RSSI) defined by the 802.11 protocol. The physical sublayer measures the energy observed at the antenna used to receive the current frame. Normally, 802.11 devices provide this value to the device driver. Besides, some card models provide information on noise as well. With these two parameters, we can estimate the Signal to Noise Ratio (SNR) for every frame received and estimate link quality between nodes, representing it with values in the $[0, max\_lq]$ range that are then treated by means of configurable moving average or median filters to eliminate noise and spurious values reported in the RSSI measurement by the wireless network card.

The calculation of the path in the ATP and MTP is based on these values. The links are divided in five categories *(no_link, bad_link, average_link, good_link, stable_link)* with different weight, being the *stable_link* the lightest and a matrix M is calculated from the LQM applying this filter. After that, the worst links are eliminated *if possible* using a simple algorithm:

```
WL = M.getWorstLink()
if WL == bad_link or WL == average_link
   M.remove(WL)
else
   exit
endif
if M.connected()
   goto 1
else
   M.restore(WL)
   M.markChecked(WL)
end if
```

Consider a connected network: the worst link WL is selected. If it is not a *bad_link* nor an *average_link* the algorith exits. On the contrary it is eliminated. If the network is still connected, the change is accepted and the algorithm restart. On the contrary the link is readmitted and the algorithm restart again. With this trivial piece of code, is possible to eliminate the worst links maintaining the network connected and selecting only the links that can give a certain guarantee on its reliability (if it is possible).

After this filter, the Dijkstra algorithm for the single-source shortest path problem for directed graphs with nonnegative edge weights is applied to the graph represented by the matrix M.

Computation time is not actually an issue (networks are usually small), since the Dijkstra algorithm has a $O(V^2)$ complexity, V being the number of vertices, whereas the implementation of the algorithm's priority queue with a Fibonacci heap makes the time complexity $O(E + VlogV)$, where E is the number of edges of the considered graph.

2.6.4 LQM Initialization

When a RT-WMP network begins, the nodes do not have topological information. Therefore, an additional step to setup the initial LQM is required. This is an easy and bounded time process in which, however, real-time behavior is not guaranteed. When a node is started, first of all the values lqm_{ij} of the LQM are all set to $lqm_{ij}^{init} = max_{lq} + 1$. In this way, all the nodes consider that they are in a fully connected network. Then, all the nodes start to listen to the medium during a *waiting period* that depends on the WMP address of each one; the lower the WMP address, the shorter the period. If during this period they hear a protocol frame, it means that there already exists an active network. In this case nodes will be incorporated in it following the procedure specified in section 2.7.2. Otherwise, at the end of the shortest waiting period, the correspondent node wakes up and

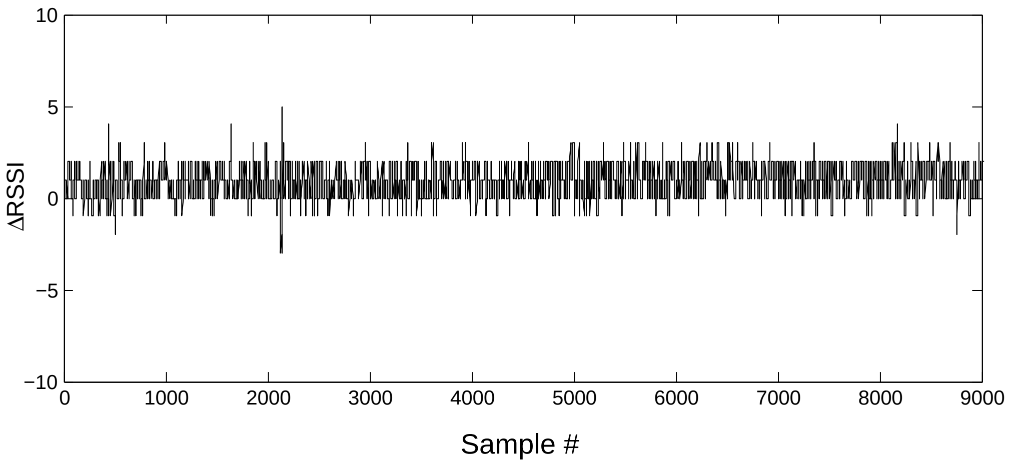


Figure 2.3: Asymmetrical behavior of links.

starts a normal PAP. Since its LQM represents a fully connected network, it chooses one of the nodes (generally starting with the one with the lowest WMP address) and sends it the token. If that node is not in its communication range, the sender will not receive the implicit acknowledgement and, after timeout, resets the corresponding value of the LQM and sends the token to another node. The process repeats up to the moment in which the token is sent to a node that is effectively in the communication range of the sender. At this moment the receiver continues the PAP in the same way assuming, however, the LQM is partially updated by the first node. The propagation of the token continues in the same fashion up to the moment in which the nodes share a real LQM. The lack of implicit acknowledgement and the timeout on the validity of the LQM elements, in fact, will rule out inexistent links.

As mentioned, the process has a bounded duration (equal to LEVP). However, it can be considered concluded when no lqm_{ij}^{init} values are present in the shared LQM.

2.7 Error Handling

The RT-WMP provides The error recovery mechanisms of RT-WMP have been designed not to jeopardize real-time behavior of the protocol and to maintain the network temporization in the majority of possible situations of error.

2.7.1 LQM Misalignment

Even if nodes receive the complete LQM frequently, sometimes a slight misalignment of the LQM can occur due to the fact that links are not usually completely

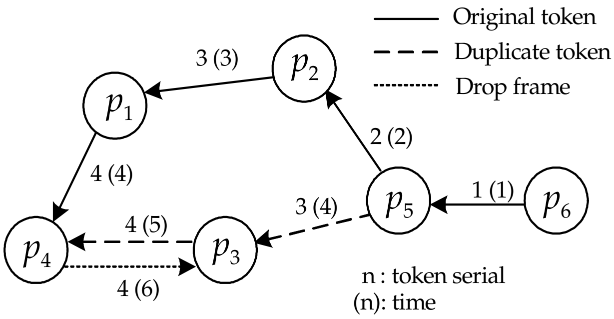


Figure 2.4: Token duplication resolution mechanism. In case of message or authorization duplication the mechanism works in a similar way.

symmetric. Figure 2.3 shows the raw difference between the RSSI ($\Delta RSSI$) registered by a pair of fixed nodes communicating with each other at a distance of about 150 m. After filtering, the difference is usually very small but it is not always negligible. This can lead to slightly different matrices in different nodes. If these differences cause a different categorization of the links in terms of weights within the LQM (see section 2.6.3, undesired behavior can take place during the routing.

Let us consider the case in which p_k, p_a, p_b can hear each other and that p_k has to send a message to a fourth node p_c that only p_a and p_b can hear. When p_k computes the path, it considers that the best is, for example, p_a, p_k, p_c. However, when the message reaches p_a, the latter considers, due to a small misalignment of the LQMs among nodes, that the safer path is p_b, p_c and instead of passing the message directly to p_c, it passes it back to p_b. In the same way, p_b can consider, instead, that the safer path is p_a, p_k. In this situation, the p_a and p_b nodes would pass the message to each other indefinitely.

To avoid this situation, during both authorization and message delivery, when a node receives a frame, it sets its corresponding bit in the *nyr* field before propagating it. The receiving node applies the mask constituted by the string of bits to the LQM setting $lqm_{ij} = 0$ and $lqm_{ji} = 0$ being i the local node and j the node corresponding to the set bit.

With the additional step just described, when p_b receives the message for the first time, it discards the possibility of sending the message back to p_a avoiding, in fact, the possibility of infinite loops and guaranteeing the upper bound of $n - 1$ hops even in the event of misaligned LQMs.

2.7.2 Node Failure or Node Loss

RT-WMP is quite robust in case of node failure. The *implicit acknowledge* technique used dispenses with the necessity of monitoring nodes to control the loss of the token. In fact, in common token-pass systems with explicit acknowledgement, when a node receives a token, it acknowledges the sender with a message. However, if a node fails just after the acknowledgement, the token is lost and a technique to regenerate it is required. In RT-WMP, however, when a p_k node sends a frame of any type, it listens to the channel for a timeout. The receiver p_l node immediately processes the frame received and sends another frame to a third p_m node (that can be its predecessor as well). The first sender listens to such a frame as well and interprets it as an acknowledgement. This technique permits saving of bandwidth and eliminates the need for a monitor node. In any case, if the first sender does not hear the frame within timeout, it supposes that the p_l node has failed or is out of its coverage range. In this case, the behavior depends on the phase that the protocol is in. If it is in the ATP or MTP, p_k discards the frame and starts a new PAP. In fact, it is impossible to calculate another path since this could jeopardize the temporization of the network (see section 3.1.1). However, if it is in the PAP, p_k node sets the $nstat[l]$ field to *reached*, modifies the local LQM and the LQM carried by the token to exclude the p_l node from the set of its neighbors (setting $lqm_{kl} = 0$) and continues with the PAP, sending the token to another node. This solution excludes the p_l node in the current PAP to preserve network temporization but not necessarily in the next PAP. In fact, it may be that there are other nodes which consider p_l to be their neighbor. If p_l has not actually failed but, for instance, has moved away from p_k node but not from another neighbor p_m, the latter will reinsert p_l in the next PAP by simply passing it the token with no additional cost. If, however, the node is actually broken or has moved away from all the other nodes, in the next PAPs all its neighbors will try to pass the token to it one after another (one in each PAP) until p_l is isolated. When this occurs, the node that starts the next PAP marks this node as *lost* setting $nstat(l) = lost + r$ where r is a number between 0 and $n-1$ and p_r does not belong to the set of lost nodes.

Reinsertion of lost nodes.

The number r represents the identity of the node that has to *search* for the lost node in the current PAP. Nodes, in fact, could reappear, but it is impossible to predict where. Consequently, nodes that still belong to the network organize themselves to search for the lost node one after another in the successive PAPs. When p_r node receives the token, it looks at the *nstat* array. If one of the elements contains the value $lost + r$, (in this case $nstat[l] = lost + r$), it tries to send the token to p_l. If the latter (implicitly) acknowledges the frame (i.e. passes the token to another node or back to p_r), it is reinserted in the network with no additional cost. Otherwise, (i.e. p_l node does not acknowledge) node p_r sets $nstats(l) = searched + r$ and continues the PAP. None of the other nodes try to search for that node in the current PAP, since this would break the network temporization (see 3.1.1 for details). The node that starts the next PAP modifies the field *nstats* to $nstats[l] = lost + ((r+1)\ mod\ n)$ if $p_{(r+1)\ mod\ n}$ node is not a lost node and continues the PAP. In this manner all the nodes not lost will search for the lost node one after another in the successive PAPs until reinsertion of the node takes place. This mechanism works with more than one lost node in the same way.

2.7.3 Frame Duplication

Communication errors can produce another type of problem. Let us consider the situation where, in the PAP, the p_k node sends a token to the p_a node and waits for an implicit acknowledgment. Node p_a processes the frame and sends the frame to node p_b. As explained earlier, the last pass is also the acknowledgement for p_k. However, if node p_b hears the frame but p_k does not, a token duplication occurs. In fact, p_k marks the node as *reached* (like in the case of a failed token-pass explained earlier) and continues the PAP by sending the token to another node. Node p_b continues the PAP as well and at that moment there are two tokens in the network. To solve this problem we introduced the *serial* field in the frames. This field contains a value that is set to zero when the first PAP begins. Before each transmission, the sender node increases this value, saves it locally, and then transmits. However, when a node receives a frame with a *serial* lower to or equal than the *highest* serial that it has transmitted, it discards the frame and informs the sender by sending a *drop* frame to it. In figure 2.4 an example situation is presented. *authorization* or *message* duplication can occur in the same way. In keeping with the behavior described earlier, the unacknowledged node discards the *message* or the *authorization* and creates a new *token* frame. However, the receiver of the authorization/message continues to route the frame along the path. At that moment there are two distinct types of frame traveling in the network. Just as in the case of a simple token duplication, though, the first node that receives a frame with an old *serial* (either token or authorization/message) will discard it.

2.7.4 Frame Retransmission

To have the possibility of guaranteeing a higher error endurance, in the current version of the RT-WMP protocol, a possibility of frame retransmission has been implemented. When a node sends a frame but does not receive an implicit acknowledgment within timeout, it can reattempt the transmission a fixed number of times. However, the use of this capability can provoke, in some situations, similar problems to frame duplication. Let us consider the situation in which p_k node sends a frame to the p_a and the latter to p_b. If p_k node does not hear the acknowledgement , it will reattempt the transmission to p_a that will receive a duplicated frame that should not propagate. In this case p_a recognizes that it is the same frame looking at the *serial* and *retry* fields and send a *drop* frame back to the p_k node that is informed, in this way, that it must discard the frame. On the other hand, this capability alters the real-time timing of the protocols (see section 3.1.2) and must be considered at the planning time since each transmission can entail n retransmissions.

2.8 Conclusion

In this chapter, we have presented the basic features of the RT-WMP, which is a novel protocol for MANETs real-time applications. It can work over commercial low-cost 802.11-protocol based networks providing real-time traffic support. It uses a token-passing scheme to guarantee bounded transmission times and has message priority support. The protocol deals with frequent topology changes through the sharing of matrices that describe link quality amongst nodes. In addition, it implements an built-in error recovery and correction mechanism that deal with token loss, token duplication and node reincorporation after a single or multiple failure. These features are implemented while maintaining real-time behavior in the most frequent error situations.

In the next chapters we will show the analysis, the evaluation and the application in real experiments of the protocol.

Chapter 3

RT-WMP: Evaluation and Analysis

In real-time protocol evaluations, a careful analysis of the performance is more than ever necessary in order to determine the effectiveness of the system and to verify a priori that the timing requirements are met in all circumstances.

The literature provides plenty of examples of performance evaluation and analysis of communication protocols. However, the vast majority of protocols are proposed and tested in simulation environments only. These include NS2 [NS2 11], Opnet [Opnet 12] or OMNeT [OMNeT 12]. Although these environments allow preliminary results to be obtained in a short time and different protocols to be easily compared, simulation results are frequently inconsistent with the real behavior of protocols, especially in wireless environments where interference is much higher than in wired networks.

In this chapter we present an evaluation and analysis of the RT-WMP protocol described in the previous Chapter 2. Several tests have been conducted in order to analyze the general performance of this protocol, its real-time features evaluated both by a theoretical analysis and using a real testbed, and its mobility capabilities. Furthermore, a comparison is made with a general purpose protocol.

On the other hand, to be used in a real real-time system a protocol must be susceptible to rigorous analysis. An in-depth analysis is carried out to examine the possibility of using such a protocol as a communication framework in a distributed real time system, taking into account issues such as the planning of tasks and resources, compliance of timing requirements, and controlled overload.

This contribution has been developed within the framework of the TESSEO Spanish National Project. The work has been submitted for publication in the Ad Hoc Networks international journal [Tardioli 13] and is currently under revision.

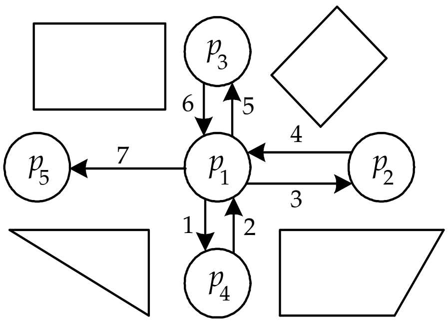


Figure 3.1: Worst case PAP situation.

3.1 Real-Time Features

In a real-time distributed system, priority support and bounded end-to-end delay is required for scheduling and time constraint guarantees. Consequently, each event/phase in a real-time network protocol *must* have a *bounded* and *known* duration.

3.1.1 Phases Boundness

The RT-WMP fulfils these requirements, since each phase has a bounded and known duration, even in the presence of the majority of errors. The PAP lasts, in the worst-case, $2n-3$ hops (see figure 3.1). In fact, if the network is connected, a covering tree with $n-1$ arcs can always be found, so the tree can be covered by visiting all its nodes two times at the most. That would mean $2n-2$ hops, but a return to the first node can be avoided; therefore, there are only $2n-3$ hops. Besides, in error situations, such as node failure or node reinsertion (or loss), this phase has *the same* duration, since the time wasted on a failed token pass can be equated to the time needed to send and return a token. Let us consider an example. Suppose that p_k is the only neighbor of p_a. In the normal functioning of the protocol, if node p_k sends the token to p_a, the latter shall pass the token back to p_k to continue the PAP. However, if node p_a is broken, after the pass node p_k will wait for a timeout and then continue with the PAP passing the token on to another node. In fact, the time spent in the first and second scenario is the same, since the timeout is equal to the time that node p_a needs to return the token. Frame duplication is the only situation that can temporarily jeopardize real-time behavior of the network due to the possibility of collisions and the need to send drop frames. In any event, the duration of this situation is limited since the first node to receive an old frame discards it and informs the sender that its frame is old.

In the ATP and MTP, the path is determined using the well-known Dijkstra algorithm (see section 2.6.3 for details). According to this algorithm, if the network

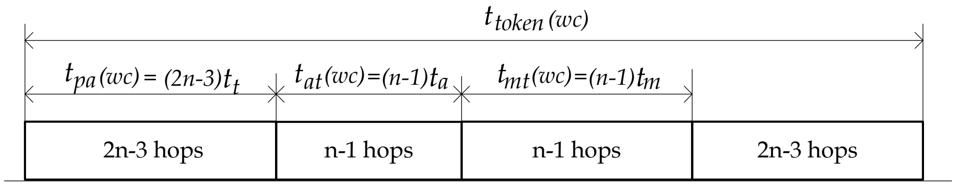


Figure 3.2: Timing of the protocol.

is connected, the maximum number of hops to go from one node to another is $n-1$. Thus these phases have a bounded duration as well. However, in case of node failure or loss during these phases, nodes shall discard the authorization or the message in order not to jeopardize the temporization of the network. For example, let us suppose that p_k node calculates a $n-1$ *hops* path to reach destination node p_d. If one hop along the path fails, for instance p_a to p_b, p_a node might find another path to reach p_d. Unfortunately, it may also occur that the sum between the number of hops already made and the number of hops of the new path is greater than the allowed maximum, that is $n-1$.

3.1.2 Timing and Bandwidth

From the global point of view, the phases of the protocol repeat one after another, as we can see in figure 3.2 with worst-case durations $t_{pa}(wc) = (2n-3)t_t$ for the PAP phase, $t_{at}(wc) = (n-1)t_a$ for the ATP and $t_{mt}(wc) = (n-1)t_m$ for the MTP, t_t being the duration of a *token* pass, t_a the duration of an *authorization* pass and t_m the duration of a *message* pass.

Timing

The *worst-case loop* can thus be defined as:

$$t_{loop}(wc) = t_{pa}(wc) + t_{at}(wc) + t_{mt}(wc) \tag{3.1}$$

Also is possible calculate that an upper bound on the interval between two consecutive receptions of a token can be expressed as:

$$\begin{aligned} t_{token}(wc) &= 2t_{pa}(wc) + t_{at}(wc) + t_{mt}(wc) \\ &= t_{loop}(wc) + t_{pa}(wc) \end{aligned} \tag{3.2}$$

Intuitively, this occurs if a node starts a worst-case PAP (in which it does not receive the token back) and has to wait for the completion of the subsequent worst-case ATP and MTP, and receives again the token after the last hop of an additional worst-case PAP.

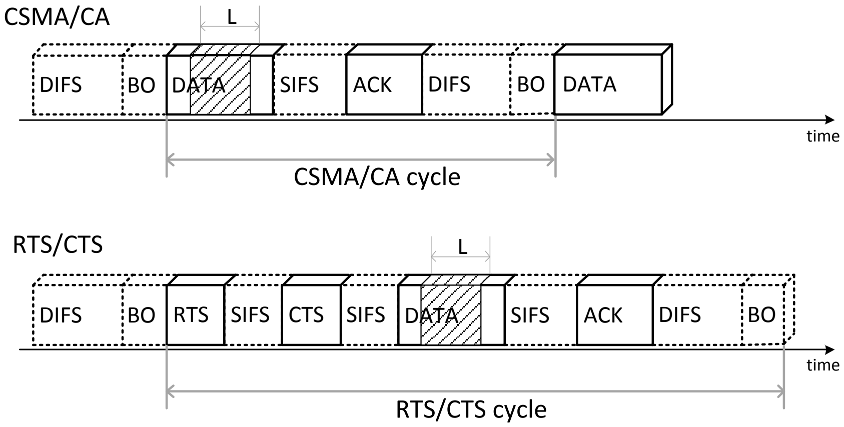


Figure 3.3: The 802.11 protocol timing.

On the other hand, the highest priority message in the network (if it is the only one) could suffer a worst-case delay of:

$$\begin{aligned} t_{ete}(wc) &= t_{token}(wc) + t_{at}(wc) + t_{mt}(wc) \\ &= 2 \cdot (t_{pa}(wc) + t_{at}(wc) + t_{mt}(wc)) \\ &= 2 \cdot t_{loop}(wc) \end{aligned} \tag{3.3}$$

Again, this can occur when the node that holds the most priority message is the PAP beginner of the situation described above and the message enters the queue just after its token pass. In that case it can occur that the message has to wait for a complete $t_{token}(wc)$ period plus additional worst-case ATP and MTP. This expression represents the maximum priority-inversion delay also, since lower-priority messages can not be preempted during an already started loop.

Bandwidth

With the temporization just expounded we can easily calculate the worst-case theoretical (end-to-end) bandwidth offered by the protocol as follows:

$$BW(Mbps) = \frac{MTU \cdot 8}{t_{pa}(wc)(\mu s) + t_{at}(wc)(\mu s) + t_{mt}(wc)(\mu s)} \tag{3.4}$$

3.1.3 Theoretical Analysis

The numerical values of these functions, depend on the configuration of the underlying 802.11 protocol and, as will be show later, on the data rate used.

Figure 3.3 shows in a simplified form how data packets are transmitted in the 802.11 protocol. The T_{DATA} is the time needed to send the payload L and the additional data (preamble, etc.), T_{SIFS} the Short InterFrame Space, T_{ACK} the time needed to send the acknowledgement, T_{DIFS} the duration of the Distributed InterFrame Space and T_{BO} the minimum backoff time mentioned in 2.1. The time $T_{802.11}$ needed to send a frame is then:

$$T_{802.11}(L) = T_{DIFS} + T_{BO} + T_{DATA}(L) + T_{SIFS} + T_{ACK} \tag{3.5}$$

when the RTS/CTS mechanism is not used and:

$$\begin{aligned} T_{RTS/CTS}(L) = T_{DIFS} + T_{BO} + T_{RTS} + T_{SIFS} + T_{CTS} + \\ T_{SIFS} + T_{DATA}(L) + T_{SIFS} + T_{ACK} \end{aligned} \tag{3.6}$$

The RT-WMP protocol does not need explicit acknowledgement (uses implicit) nor backoff mechanisms or RTS/CTS frames (the token passing technique used avoids the need for collision avoidance mechanisms) and the trasmission scheme of a single RT-WMP frame is simplified in this manner:

$$T_{RT-WMP}(L) = T_{DIFS} + T_{DATA}(L) \tag{3.7}$$

being L the length of each one of the frames to be sent. This approach guarantees a more efficient raw use of the available bandwidth. However RT-WMP is a three phases protocol and to deliver a data message needs to send several additional frames. The T_{RT-WMP} should be thus written as:

$$\begin{aligned} T_{RT-WMP}(L) =& h_{PAP} \cdot [T_{DIFS} + T_{DATA}(stoken)] + \\ & h_{ATP} \cdot [T_{DIFS} + T_{DATA}(sauth)] + \\ & h_{MTP} \cdot [T_{DIFS} + T_{DATA}(smessage + L)] \end{aligned} \tag{3.8}$$

being h_{PAP}, h_{ATP}, and h_{MTP} the number of hops of the correspondent frame in the PAP, ATP and MTP respectively, *stoken*, *sauth* and *smessage* the size of a token, authorization and message frame respectively.

The values of all the mentioned 802.11 elements (T_{DIFS}, T_{ACK}, etc.) depend on the network data rate and on the modulation technique used (see [Jun 03] for more details) but has a strong influence on the efficiency ϵ of the 802.11 networks defined as:

$$\epsilon = \frac{TMT}{R} \tag{3.9}$$

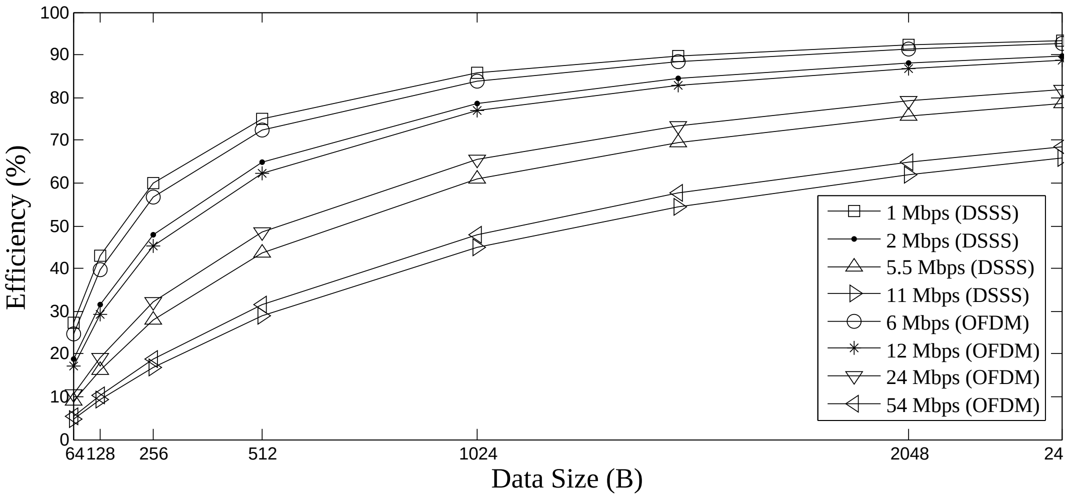


Figure 3.4: Efficiency of a RT-WMP five-nodes completely connected network.

being TMT the Theoretical Maximum Throughput (TMT) and R the declared network rate introduced in [Jun 03].

Similarly the efficiency of RT-WMP depends on these parameters and additionaly on the network size since both h_{PAP}, h_{ATP}, h_{MTP} and the size of *stoken* dependent on this parameter. A simple analysis can discover the behavior of the RT-WMP protocol. Figure 3.4 shows the efficiency of a sample completely-connected five-nodes network as a function of the data rate. Adding further nodes to the network will not alter the shape of the graph but will provoke an increment on the convexity of the curves. In any way, as in standard 802.11 networks, the lower the rate the higher the efficiency. Once fixed a sample data rate of 6 Mbps (for being, in our opinion, the best compromise among bandwidth, efficiency and communication range) is it possible to provide concrete values for all RT-WMP characteristics. For this data rate the 802.11 protocol specifies: $T_{DIFS} = 34$ while

$$T_{DATA}(L) = 20 + 4 \cdot \frac{22 + 8 \cdot (34 + L)}{24}(\mu s) \tag{3.10}$$

Using this expression it is easy to calculate:

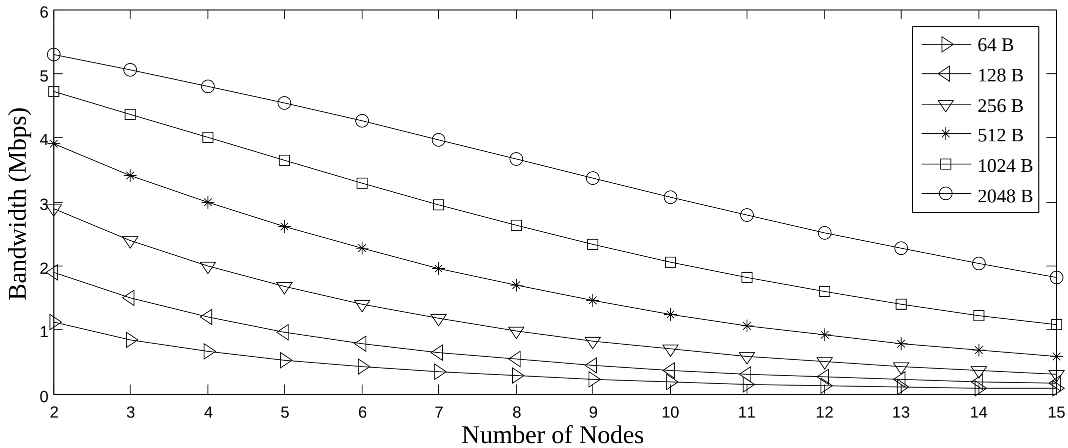


Figure 3.5: Worst-case bandwidth offered by RT-WMP.

$$t_{token}(\mu s) = T_{DIFS} + T_{DATA}(stoken) \\ = 34 + 20 + 4 \cdot \frac{22 + 8 \cdot (34 + stoken)}{24} \mu s \tag{3.11}$$

$$t_{auth}(\mu s) = T_{DIFS} + T_{DATA}(sauth) \\ = 34 + 20 + 4 \cdot \frac{22 + 8 \cdot (34 + sauth)}{24} \mu s \tag{3.12}$$

$$t_{msg}(\mu s) = T_{DIFS} + T_{DATA}(stoken) \\ = 34 + 20 + 4 \cdot \frac{22 + 8 \cdot (34 + smessage + L)}{24} \mu s \tag{3.13}$$

These values allow the calculation of all the parameters defined in section 3.1.2. Table 3.1 shows the values for different number of nodes and frame size and network configuration. Figure 3.5.a and b show the theoretical maximum throughput for a completely connected network and a worst-case network respectively. Figure 3.6.a shows the relative efficience $\epsilon_r^{802.11}$ defined, for a completely connected network, as:

$$\epsilon_r^{802.11} = \frac{TMT_{RT-WMP}}{TMT_{802.11}} \tag{3.14}$$

being TMT_{RT-WMP} the TMT for a RT-WMP network and $TMT_{802.11}$ the TMT for a standard 802.11 network. Finally figure 3.6.b shows the *relative efficience* $\epsilon_r^{RTS/CTS}$ defined, for a worst case network, as:

$$\epsilon_r^{802.11} = \frac{TMT_{RT-WMP}(wc)}{TMT_{RTS/CTS}(n-1)^{-1}} \tag{3.15}$$

being $TMT_{RT-WMP}(wc)$ the worst case TMT for a RT-WMP network and the term $TMT_{RTS/CTS}(n-1)^{-1}$ the TMT for a standard 802.11 network using the RTS/CTS mechanism adapted for a n nodes network without spatial reuse. These two last graphs show how much the RT-WMP takes advantage of the available theoretical maximum bandwidth offered by the plain RT-WMP. The results are very interesting especially considering the worst-case situation which is that must be considered at planning time as explained before. The RT-WMP can in fact maintain efficiencies that are above 40% even for relatively big networks (up to 15 nodes). It is important to notice the results do not take into account any routing protocol that, however, must be used on top of the plain 802.11 to allow it to support multi-hop communication and that should add additional overhead.

3.1.4 Testbed

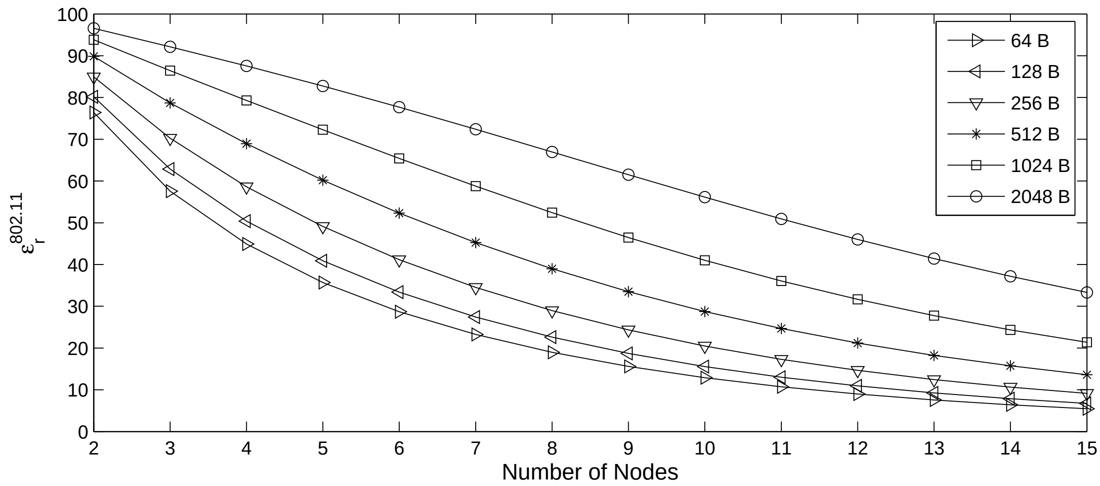
The RT-WMP has been implemented to work in different platforms. It can work as a standalone user-space Linux program (the specific application can be linked with the RT-WMP core library), as a module of the Linux Kernel (it provides a set of APIs to communicate with it and also provides virtual interface to the user) and as a library for the real-time operating system MaRTE OS [Rivas 01]. Both the Linux and MaRTE OS implementations can use a dedicated wireless-card driver. This driver, called *ath5k_raw* and developed by the Robotics Perception and Real-Time Group at the University of Zaragoza, is based on the *ath5k* Linux kernel driver and is compatible with most Atheros-chipset based cards. It allows communication between peers while avoiding the use of high layer protocols (such as IP or UDP) and also avoiding MAC layer frame retransmission. It is capable of returning the RSSI level of each received frame.

To evaluate the real-world performance of the RT-WMP, we used the MaRTE OS implementation running on up to 10 nodes equipped with PC Engines ALIX.2D3 System Board with a 500 MHz AMD Geode LX800 CPU, 256 MB RAM and one Engenius EMP-8603 dual band Atheros-based wireless card node running the MaRTE OS version of the RT-WMP. An extra Linux machine was used to sniff the wireless medium, collect the information and analyze the results. Moreover, in the mobility management experiments, we used a MobileRobots' Pioneer P3AT mobile robot equipped with an onboard Versalogic VSBC-8 PC board (Pentium III at 800 MHz) and an atheros based wireless card. The wireless card frequency was fixed at 5.2 GHz and the data rate at 6 Mbps in all the experiments. In all the experiments the collision domain was free of foreign network interference.

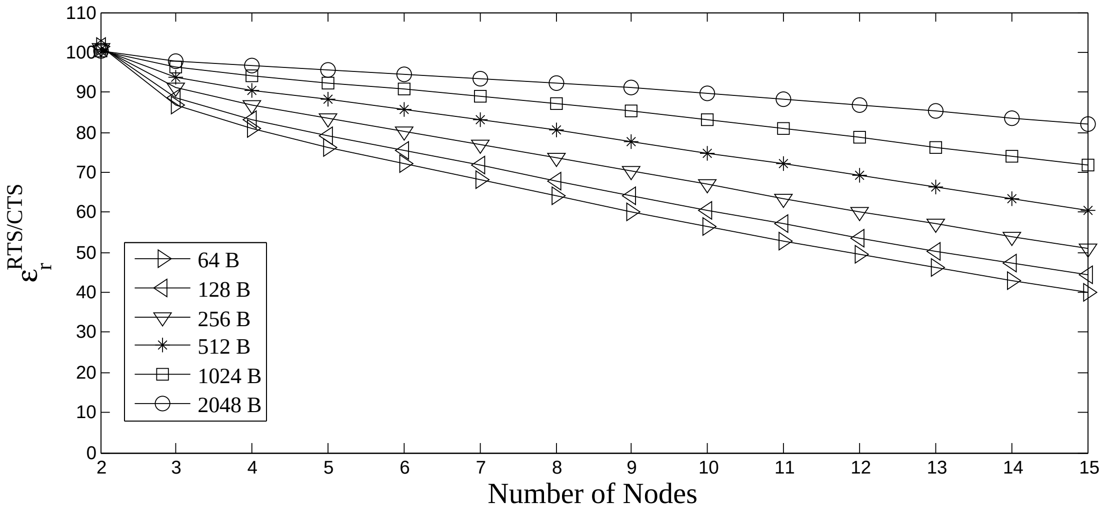
The experiments were oriented to verifying and analyzing different aspects. In the following paragraphs the evaluation of the worst-case real-time behavior and throughput is presented. Moreover, the results of additional outdoor experiments are shown to demonstrate the efficient management of the mobility.

	2 Nodes			3 Nodes			4 Nodes			5 Nodes			10 Nodes		
Size	64	512	1500	64	512	1500	64	512	1500	64	512	1500	64	512	1500
t_t	0.131	0.131	0.131	0.139	0.139	0.139	0.149	0.149	0.149	0.163	0.163	0.163	0.269	0.269	0.269
t_a	0.119	0.119	0.119	0.119	0.119	0.119	0.119	0.119	0.119	0.119	0.119	0.119	0.119	0.119	0.119
t_m	0.209	0.807	2.124	0.209	0.807	2.124	0.209	0.807	2.124	0.209	0.807	2.124	0.902	0.807	2.124
$t_{pa}(wc)$	0.273	0.273	0.273	0.417	0.417	0.417	0.748	0.748	0.748	1.141	1.141	1.141	4.584	4.584	4.584
$t_{at}(wc)$	0.177	0.119	0.177	0.238	0.238	0.238	0.357	0.357	0.357	0.476	0.476	0.476	1.071	1.071	1.071
$t_{mt}(wc)$	0.209	0.807	2.124	0.419	1.614	4.248	0.629	2.421	6.373	0.838	3.228	8.497	1.887	7.263	19.119
$t_{loop}(wc)$	0.459	1.057	2.374	1.074	2.269	4.903	1.734	3.526	7.478	2.455	4.845	10.114	7.542	12.918	24.774
$t_{token}(wc)$	0.591	1.188	2.505	1.491	2.686	5.320	2.482	4.274	8.226	3.596	5.986	11.255	12.127	17.503	29.359
$t_{ete}(wc)$	0.919	2.114	4.748	2.148	4.538	9.807	3.468	7.052	14.957	4.911	9.690	20.229	15.08	25.837	49.549

Table 3.1: Theoretical timing delay (ms).



(a)



(b)

Figure 3.6: Relative efficiency of RT-WMP compared with plain 802.11 protocol considering a completely connected network (a) and a network in which no spatial reuse is possible (b).

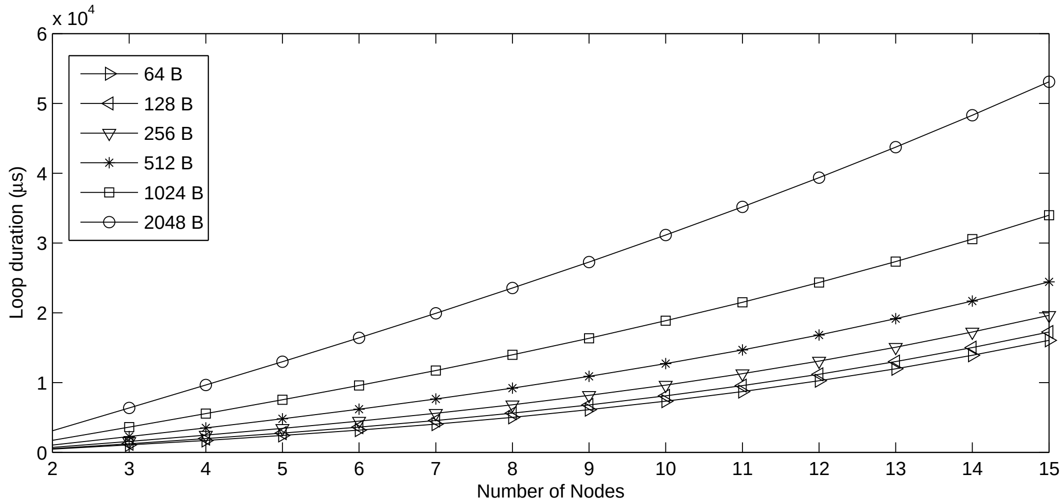


Figure 3.7: Theoretical loop duration for a worst-case RT-WMP network.

3.1.5 Real-time Behavior

A 7-node network was arranged in an indoor environment. Since the goal was to determine the worst-case behavior, we provided the nodes with a hard-coded fixed fake LQM to simulate a chain network. In this type of network, it is frequent to have worst-case loops.

Priority

In the first experiment we verified the priority-based message exchange mechanism. In the arranged network, saturated traffic with random destination and priority p ($p \in [1, 25], p \in \mathbb{N}$) and fixed-size message (1024 B) was generated in all the nodes. The messages were generated with fixed frequency and the nodes had a queue of 25 messages.

The wmpSniffer was used to sniff the medium and collect information about the messages exchanged among the nodes.

The figures 3.8 and 3.9 show the mean end-to-end delay (from the moment in which the message is pushed in the queue until the delivery to the destination node) as a function of the message priority.

Fairness

In the second experiment we verified more specifically the fairness for same-priority messages. The importance of the fairness in multi-hop networks, with special attention paid to multi-hop flows, is shown in [Szott 09].

As in the previous experiment, saturated traffic was generated in all the nodes. However, this time all the messages had the same fixed priority. Figure 3.10 shows

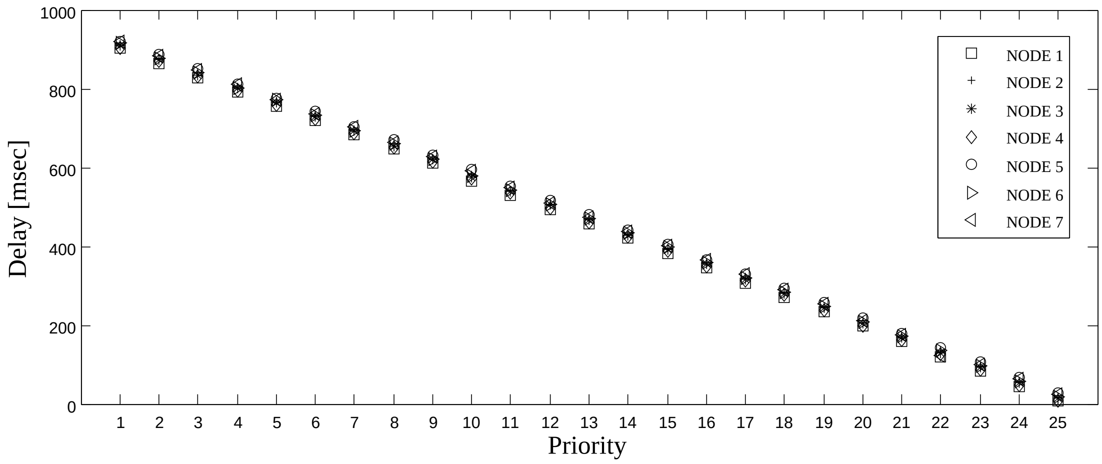


Figure 3.8: Mean end-to-end delay vs priority for a 7 nodes RT-WMP completely connected network.

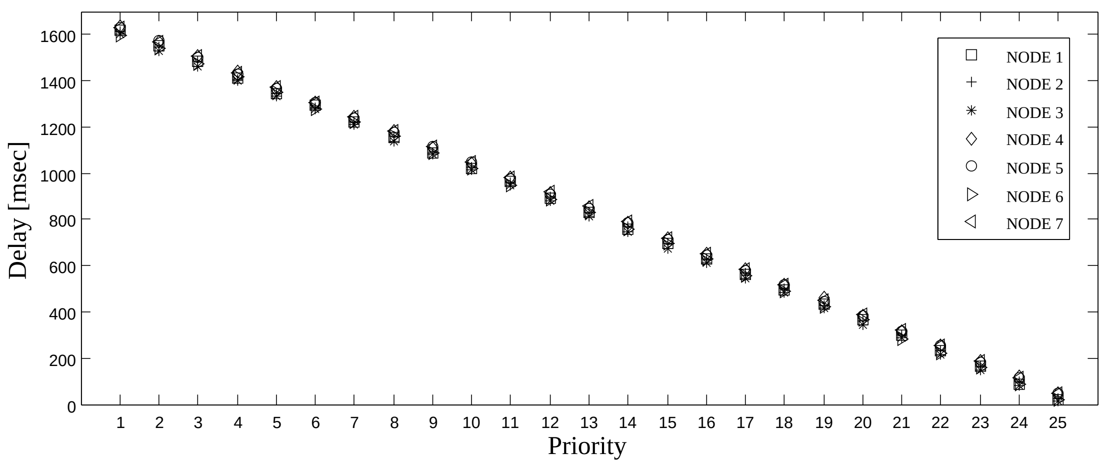


Figure 3.9: Mean end-to-end delay vs priority for a 7 nodes RT-WMP chain connected network.

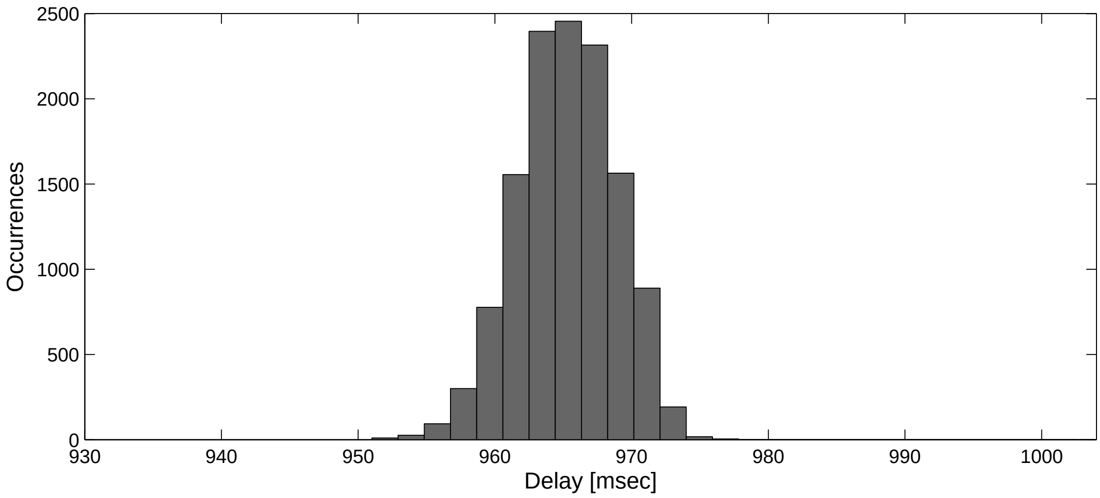


Figure 3.10: Mean end-to-end delay vs priority for a 7 nodes RT-WMP chain network.

the distribution of the delays for same-priority message for all the nodes. Again, it is possible to appreciate that all the messages suffer from a similar delay in all the nodes. The graph shows a normal distribution with a mean of 962 ms using a queue of 25 messages per node.

Notice that the raw value of the end-to-end delay for both experiments depends on the queue size and is not comparable with the values obtained in the theoretical analysis.

3.1.6 Throughput and end-to-end delay

To verify the real end-to-end throughput of the protocol we performed two types of experiments.

Completely connected network

In a first step, we arranged completely connected networks of 2 to 7 nodes. Saturated traffic with random priority and destination was generated in all the nodes. This traffic was sniffed by the wmpSniffer to measure the end-to-end delay of each message exchanged. The bandwidth was then calculated as:

$$BW = \frac{P}{t_{PAP} + t_{ATP} + t_{MTP}} \tag{3.16}$$

P being the payload of the message. The experiment was repeated for different-size messages, from 256 to 1024 bytes. Figure 3.11 shows the results of the experiment both in terms of bandwidth and end-to-end delay. This time, the values do not take into account the time spent by the messages in the queue, i.e.they only

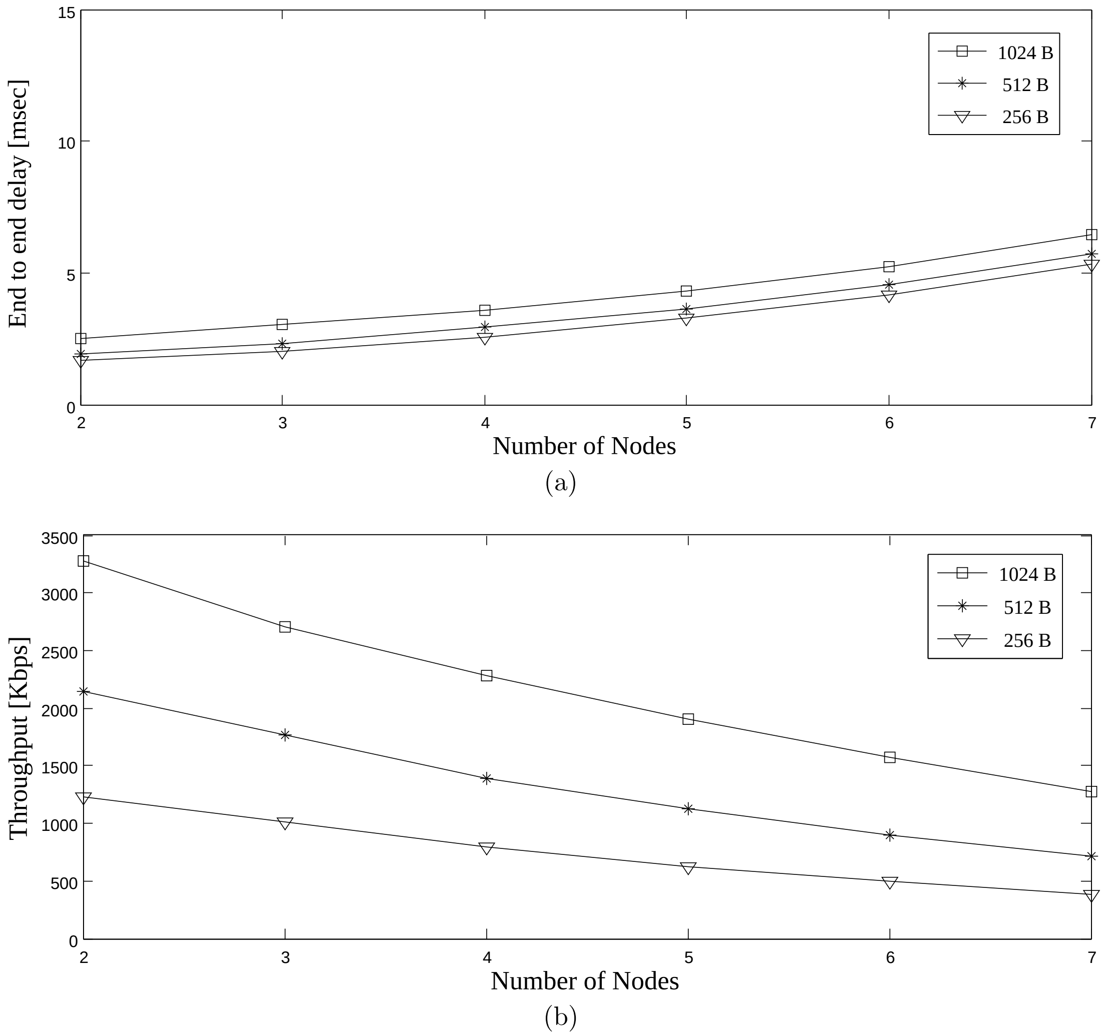
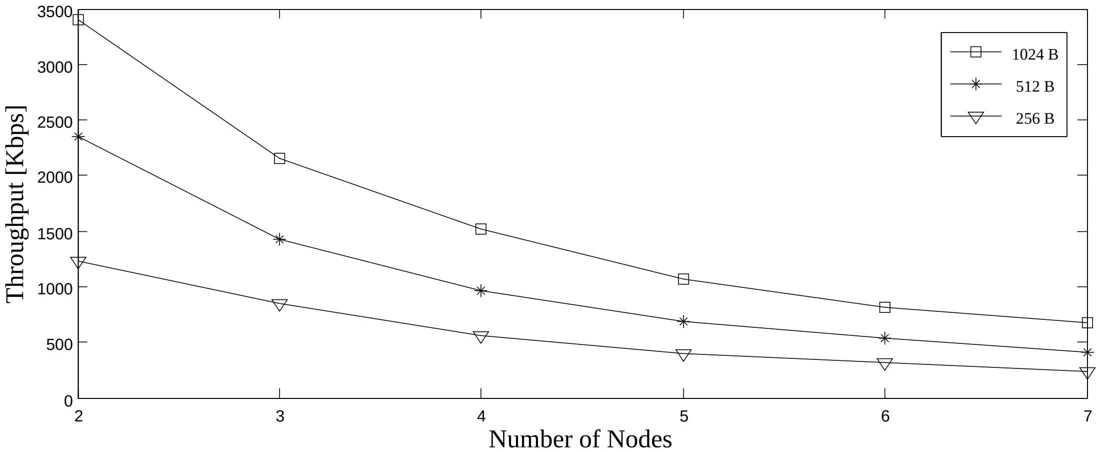
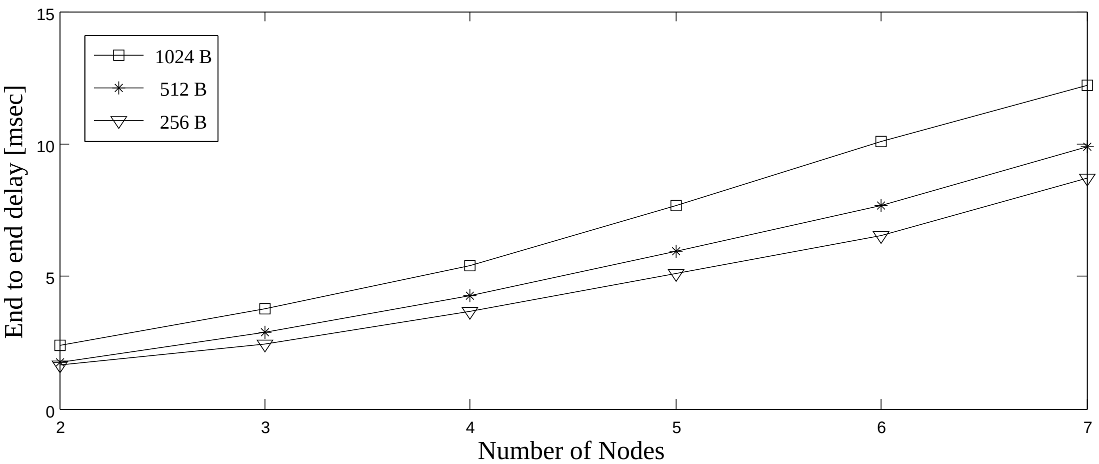


Figure 3.11: RT-WMP completely connected network Throughput and Etoe for different-size messages.

represent the time lapse between the beginning of the PAP in which a specific message is to be delivered and the moment in which the latter reaches the destination node. This means that we are cutting off the blocking time. This aspect will be addressed later both in the real-time analysis and in the subsequent experiments. These values reflect the behavior of the RT-WMP in a hypothetical situation in which all the nodes can communicate with each other. In fact, this is not of great interest from the real-time point of view (as explained before, we always have to consider the worst-case in this type of system) but it is useful to give a rough idea of the maximum bandwidth that RT-WMP can offer if used as a normal multi-hop protocol. The results are similar to those obtained in the theoretical analysis even though a worse behavior can be observed due to the computation time that, as for the 802.11 protocol, was not considered.

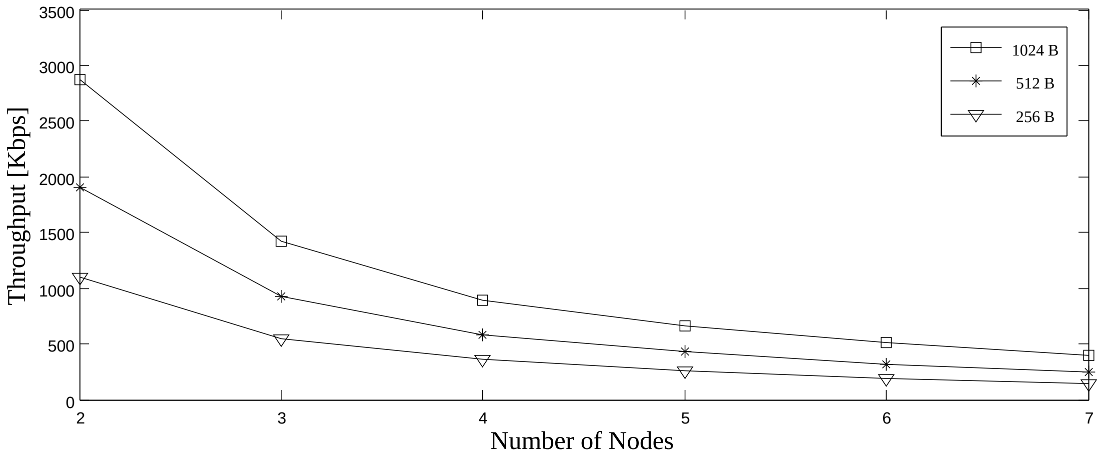


(a)

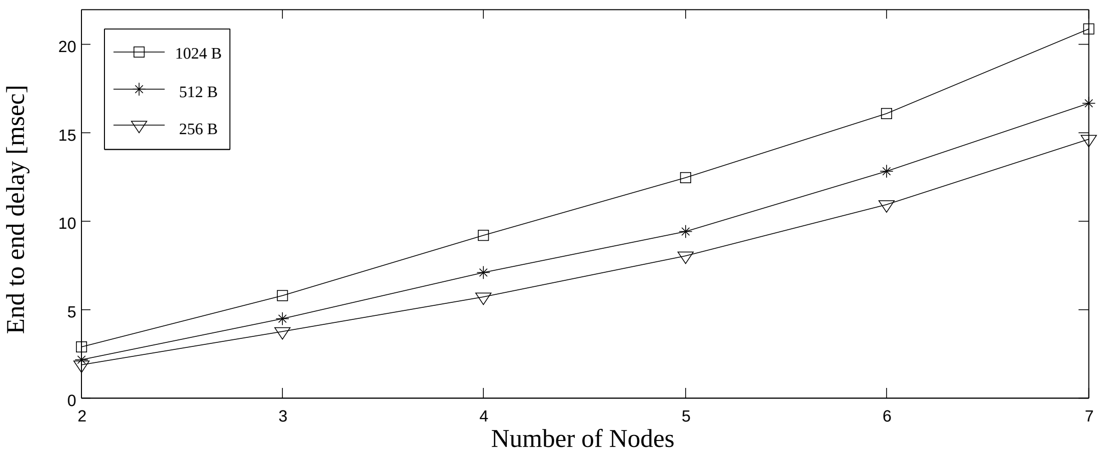


(b)

Figure 3.12: RT-WMP chain network throughput and etoe for different-size messages.



(a)



(b)

Figure 3.13: RT-WMP worst case network throughput and etoe for different-size messages.

Figure 3.14: Scenario of the experiment.

Worst-case networks

In the second step, our goal was to measure the mean and the worst-case performance of the RT-WMP in a worst-case network configuration. Moreover, in an additional experiment we measured the blocking time suffered by maximum priority messages when inserted in a network saturated by lower-priority messages.

To do this, we arranged a 2 to 7 node chain network in an indoor environment. As commented earlier, worst-case loops can in fact occur frequently in this type of network. As in the experiment mentioned above, we provided the nodes with a fake LQM to simulate a pure chain network (nodes can only communicate with their immediate neighbor).

Also in these experiments, saturated traffic with random destination and priority was generated in all the nodes. The wmpSniffer was used to collect information about the traffic exchanged. Figure 3.12 shows the mean behavior of the protocol. This figure shows the mean end-to-end delay suffered by the messages and the bandwidth offered during the experiments as a function of the message size. Figure 3.13 shows instead the worst-case end-to-end and bandwidth, the latter calculated as in eq. 3.16 when $t_{PAP} = t_{PAP}(wc)$, $t_{ATP} = t_{ATP}(wc)$ and $t_{MTP} = t_{MTP}(wc)$.

The results are very similar to those predicted by the theoretical analysis even if, again, the computation time is not negligible.

3.1.7 Mobility management

The management of the mobility is a key strength of the RT-WMP. To verify its behavior in this respect, we carried out an experiment in an outdoor environment that involved a total of 5 nodes.

We arranged 4 nodes in a straight line at about 25m distance from each other to obtain a chain network. The nodes were configured at 5.2 GHz (IEEE 802.11a band) to avoid interference and at a rate of 6 Mbit/s. The transmission power was fixed at 10 dbm and an attenuator of 20 dB was used in all the nodes. In this way we obtained an effective transmission of -10 dbm that allowed a network topology very similar to a pure chain. A mobile robot with an onboard node (see figure 3.14) was then moved at slow speed from near the first node (n_1) to a little beyond the last node (n_4) of the chain, through a straight line parallel to the line intercepted by $n_1..n_5$. During this movement, the serial number of the message, the identity of the node that delivered the message and the corresponding RSSI were recorded.

The objective of the experiments was to move the mobile robots along the whole chain (backbone) network without losing network connectivity and to observe the reaction of the protocol in a changing topology. Our goal was to obtain statistics from these data about the number of lost messages and the behavior of both protocols in terms of mobility management.

The figure 3.15 shows the results of the experiment. In figure 3.15.a, the markers represent the raw RSSI with which the mobile node received the messages during the experiment and which node delivered it. It is possible to observe that the RT-WMP protocol managed to maintain the RSSI over a value of 20%. Also, it is almost always the backbone node closest to the robot that delivers the message to the onboard node of the latter following, as expected, a behavior that depends directly on the signal level (and thus, with the opportune approximation, the distance). Even so, it is possible to see that in the switching points (see for example fig. 3.15.a, around $x = 70m$) the messages are delivered alternatively by two or three adjacent nodes. This is due to the fact in that points the categorization of the links is similar and the routing algorithm decides at each moment which node to use as repeater. This shows the correct behavior of the protocol that, as expected, adapts the path to the changing topology to constantly maintain the all its link at a safe value.

The distribution in figure 3.15.b presents the number of messages lost during the experiment. As shown, only 0.17% of the messages did not reach the destination, a percentage that, from our point of view, is small enough to allow a firm real-time control of many robotics systems.

3.2 RT-WMP vs OLSR

The RT-WMP is a protocol that offers a number of characteristics that general purpose routing protocols do not. Examples are priority support, mobility management and, of course, real-time support. For this reason, it may appear strange to compare the RT-WMP with this general type of protocol, but it could be useful to give a rough idea about the performance we can expect when the former is used in real applications. If we could catalog the RT-WMP as a general purpose

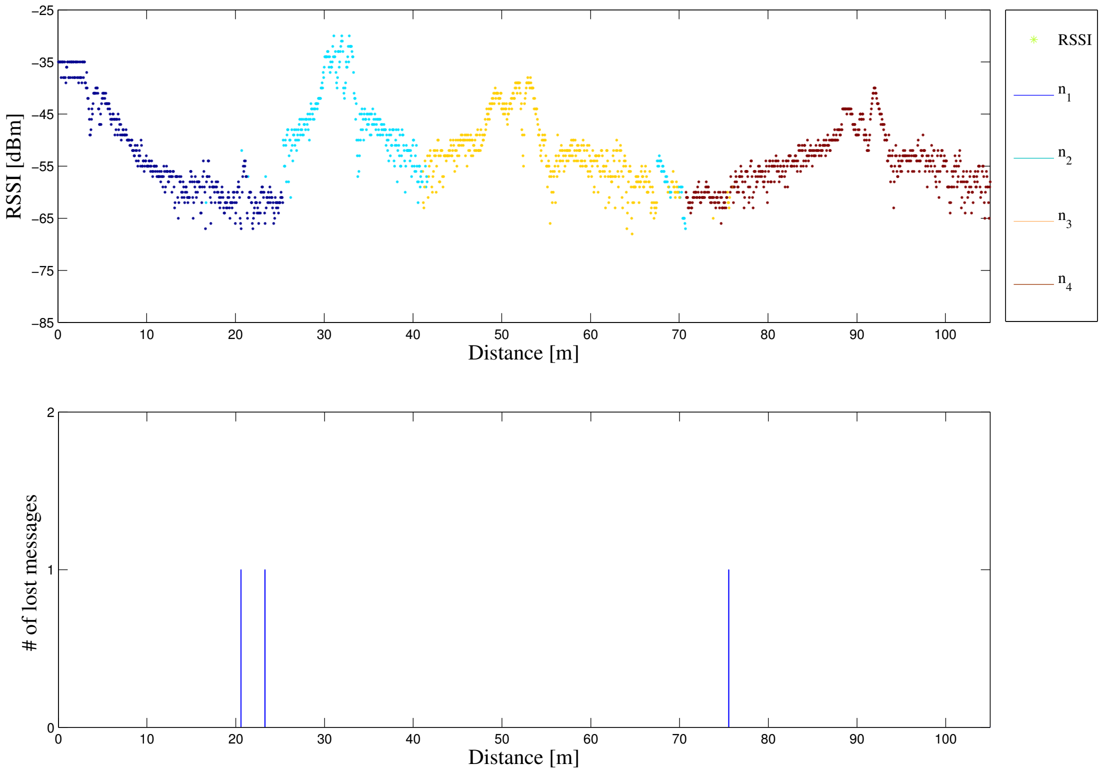


Figure 3.15: Mobility management of the RT-WMP protocol.

protocol, it would be among the proactive protocols since the routing topology information is maintained actively during communication. Furthermore, the topology maintenance is based on the link quality among nodes and the mobility is managed taking into account such qualities. Since these characteristics suggest some similarities with the Optimized Link State Routing (OLSR) protocol with the link quality extension [Jacquet 03], we decided to compare the RT-WMP with the OLSR to obtain information about its performance. It was also taken into account that, to the best of our knowledge, no similar real-time protocols have yet been implemented.

3.2.1 The OLSR protocol

To execute these experiments, we used the *unik-olsrd* implementation included in Ubuntu Linux 10.04 which supports natively the *link quality extension*. This allows the protocol to choose topologies also taking into account the link-quality, which is estimated by means of analyzing the packet error ratio. It was run over the aforementioned two to seven nodes, this time running Ubuntu Linux 10.04.

At this point, it may be helpful to point out that the OLSR maintains the topology by flooding topology information: using *Hello* messages each node discovers 2-hop neighbor information and performs a distributed election of a set of multipoint relays (MPRs). The nodes select MPRs in such a way that there is a path to each of their 2-hop neighbors via a node selected as an MPR. These MPR nodes then source and forward TC messages that contain the MPR selectors. The forwarding path for TC messages is not shared among all nodes but varies depending on the source. Only a subset of nodes source the link state information. Not all links of a node are advertised but only those that represent MPR selections. Link-state routing requires the topology database to be synchronized across the network. The OLSR simply floods topology data often enough to make sure that the database does not remain unsynchronized for extended periods of time. This means that the higher the frequency of the *Hello* messages, the more reliable the topology database. This in turn implies that if management of the mobility is required, it is necessary to increase the frequency of the topology-maintenance messages. However, this obviously increases the overhead and reduces the user-available bandwidth. In the next section, a comparison between RT-WMP and OLSR is proposed considering the results obtained when varying the *Hello* and *TC* messages.

3.2.2 Bandwidth

As explained earlier, the OLSR is not a real-time protocol and thus can not guarantee bounded end-to-end delays. For this reason we decided to compare the protocols in a common real-world *worst-case situation* and evaluate the rough bandwidth offered by both. By worst-case situation, we refer to a situation in which both protocols can work but that imposes restrictions on the operation. Specifically, we arranged a chain network of 2 to 7 nodes and measured the bandwidth available to two flows: the first between the first and the last node and the second between the last node and the first.

To force a chain network, we used the previously mentioned *fake_lqm* for RT-WMP while for the OLSR protocol, we used a modified version of the *mac80211* Linux-module that was in charge of discarding all the frames received from nodes that were not one-hop neighbour.

In both cases we obtained pure chain networks, that is to say each node could only communicate with (and listen to) its closest neighbor(s). This situation represents the worst possible scenario for both solutions since the traffic has to traverse the whole network to reach the destination node. In both cases, saturated traffic was generated at the ends of the chain. Fixed-size messages of 1024 bytes were sent as RT-WMP messages in the RT-WMP network and as UDP packets in the OLSR network.

Figure 3.16 shows the results of the experiment. It can be seen that the performance of both protocols is very similar. RT-WMP even outperforms OLSR in larger networks when the *Hello* and *TC* messages have a higher frequency. This is due to the fact that, even though the RT-WMP is a three phase protocol, it is

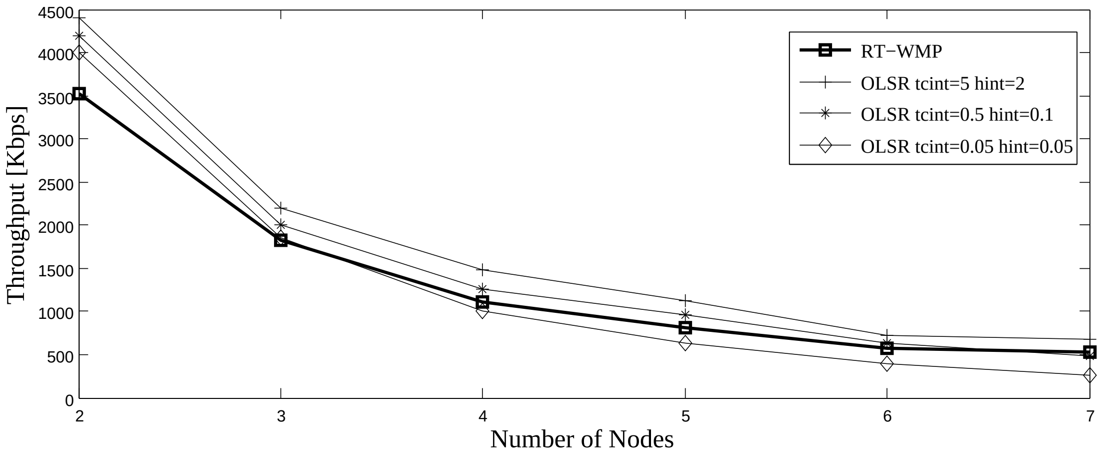


Figure 3.16: Rough bandwidth offered by RT-WMP and OLSR protocols.

more efficient for medium access since the use of the token passing technique avoids the need for collision avoidance techniques, random backoff delays, MAC-layer acknowledgements and so on. Moreover, the use of IP and UDP layers in the case of OLSR (notice that it works over IP) adds extra overheads to the communication.

3.2.3 Mobility

After testing the bandwidth, we were interested in comparing the mobility management of both protocols. We repeated the experiment described in section 3.1.7 for the OLSR protocol with the aim of comparing the results with those obtained for RT-WMP.

The figures 3.17 show the results for OLSR. In contrast to the behavior of the RT-WMP, by design the OLSR protocol responds to changes in the topology only when there is some packet loss due to the fact mentioned previously that the link quality is estimated through the PDR.

This fact is reflected in figures 3.17.a and 3.17.b. On the one hand, since the link level is not taken into account by the protocol for routing decisions, it is possible to observe that it goes below the limit of $-65dBm$ on several occasions. On the other hand, the routing algorithm does not necessarily provide privilege to the communication with the closest node and this implies that many communication switches among different nodes. In figure 3.17.a, for example, it is possible to observe a large switch between node n_1 and n_2 at approximately $x \approx 30m$. Even more evident is the switching at $x \in [75m, 90m]$ where three backbone nodes share the work of delivering the messages. These changes are cause and effect of the message losses shown in figure 3.17.b and that in the experiment reach the not negligible value of 5.34%, approximately 30 times more than the RT-WMP. Also the OLSR protocol suffered from long outages during node movement as already

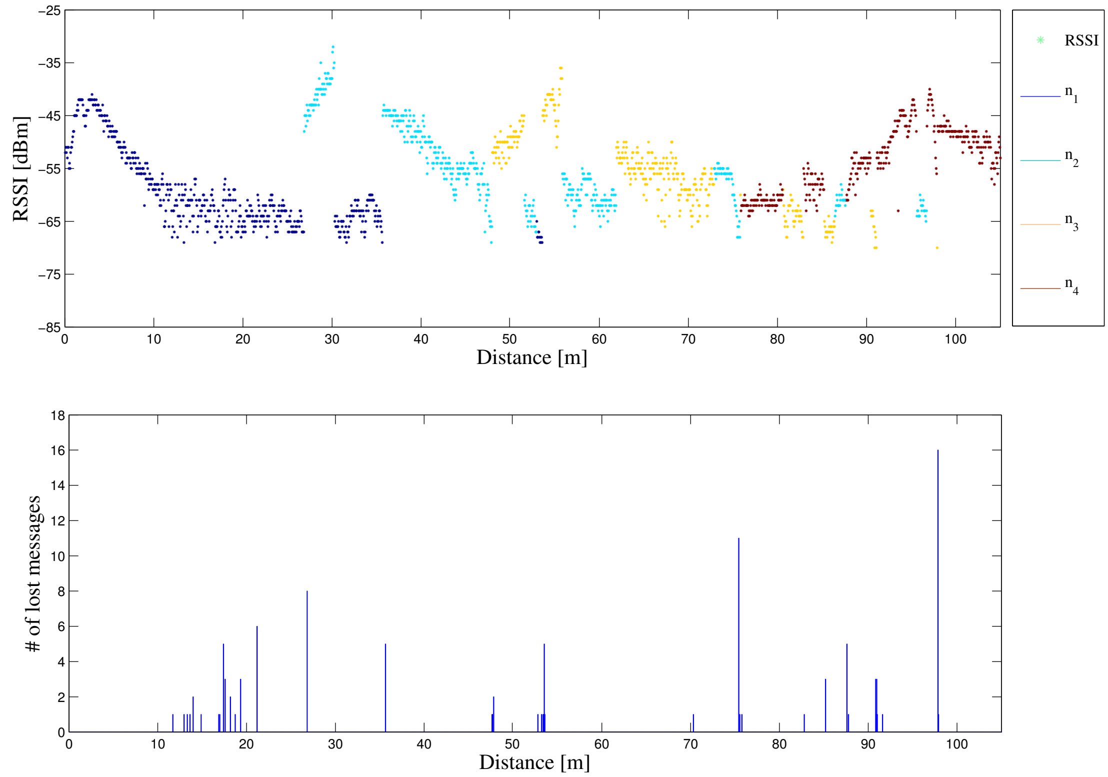


Figure 3.17: Mobility management of the OLSR protocol.

highlighted by the experiments described in [Pojda 11]. Moreover, according to the data collected, approximately 0.65% of the messages reached the destination out-of-order. This is an additional problem that is particularly evident when the frequency of sending the messages rises. These limitations suggest that it is probably not a good idea to use such a protocol in scenarios that include mobility, especially if the loss of messages is an important issue (for example in firm real-time control).

3.2.4 Lesson learned

The performance evaluation of RT-WMP has shown that it is able to support time sensitive applications even in the presence of mobility of the nodes. The comparison with a general purpose routing protocol showed, moreover, that this type of protocols can not easily be used for time-sensitive mobile applications due to the unpredictability of the end-to-end delay, to the absence of priority support and to the poor performance in terms of mobility management. On the other hand, to be used in a real real-time system a protocol must be analyzable. In the following sections we present an in-depth analysis that provides the user with the possibility of using such a protocol as a communication framework in distributed real-time systems.

3.3 Analysis of the protocol

As has been anticipated, the hallmark of a real-time system is predictability. This feature is associated with the possibility of proving or verifying a priori that the system timing requirements are met in all circumstances. As a result, predictability involves several aspects to be taken into account especially as regards careful *planning of tasks and resources*, *compliance of timing requirements* and a *controlled overload*.

Timing intervals are determined by the way the protocol works when it receives an external event (i.e. receiving a frame). Understanding the execution of a task in response to to this event can be helped by knowing the different protocol states and the interaction between them. For this reason, modeling by a finite state machine could be a simple and effective way to describe the dynamic behavior of the protocol.

On the other hand, the compliance of timing requirements could be fulfilled knowing a priori the limitations of the protocol in terms of message transmission. Message packets are non preemptible, and therefore there is a bounded *Worst case* and *Blocking* time that have to be taken into account during the analysis. In addition, the token based approach makes the protocol dependent on the number of stations, so the additional *overheads* introduced also have to be considered in the analysis.

As regards overload, the processor processing load due to the execution of the protocol has to be taken in account. The design of communication systems without Real Time requirements focuses on maximizing the throughput of the message and minimizing average delay [Tanenbaum 97]. Maximization of bandwidth might not have a high practical value if the communication overheads leave no CPU time to process the data. This aspect is even more significant in the case of embedded systems that generally have more limited processing capability. Bandwidths will decrease if protocol or application processing saturate the CPU, so processor utilization could be considered as important as other communication parameters.

In the following section, we perform a real-time analysis of the RT-WMP protocol taking in account the previous issues through a similar methodology as that presented in [Martínez 05] and [Liu 73].

3.3.1 RT-WMP as a state machine

In order to understand its functionality, each RT-WMP node can be described as a *finite state machine* (FSM). FSM provides a natural and well-understood way to describe the behavior of the protocol and to analyze the feasibility of transitions through the several states, for example by detecting abnormal network operations.

Fig. 3.18 shows the states and the transitions between them. They are briefly described below:

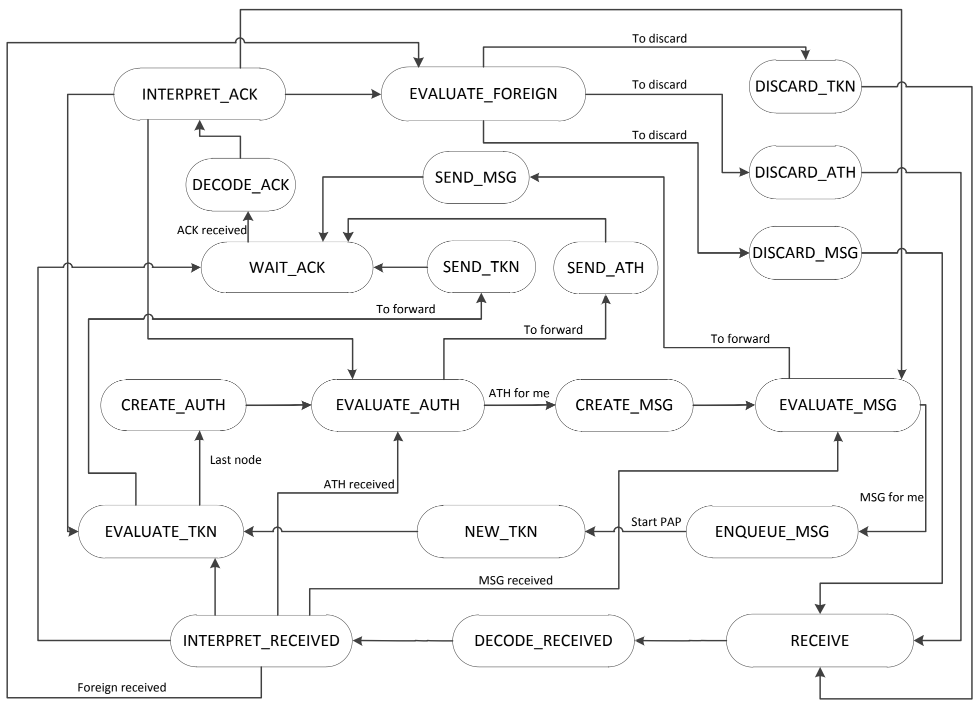


Figure 3.18: RT-WMP state machine in each node.

- $RECEIVE$: The information received is entered in the appropriate queue of the receiving station.
- $DECODE\_RECEIVED$: The node updates the LQM token field with its local data and saves the matrix locally.
- $INTERPRET\_RECEIVED$: The received frame is interpreted in order to know if it is a token, an authorization message or foreign.
- $ENQUEUE\_MSG$: The received message is written into the reception queue. It then switches to the NEW_TKN state.
- NEW_TKN: The node destination of the message initiates a new PAP phase.
- $EVALUATE\_TKN$: Updates the token if its own priority is higher and sends the token to the next station. It then switches to the Idle state.
- $EVALUATE\_MSG$: The node evaluates if it is the destination of the message.
- $CREATE\_MSG$: After receiving the authorization, the node creates the message.

- *EVALUATE_ATH*: The node checks if it is the authorization destination or not. It switches to the CREATE_MSG or SEND_AUTH state respectively.
- *CREATE_ATH*: The last node to receive the token, which knows the identity of the MPM holder, closes the PAP and initiates the ATP. Then it switches to the EVA_AUTH state.
- *SEND_TKN*: The node sends the token and switches to the WAIT_ACK state.
- *SEND_ATH*: The node sends the authorization and switches to the WAIT_ACK state.
- *SEND_MSG*: The node sends the message and switches to the WAIT_ACK state.
- *WAIT_ACK*: The station listens for the arrival of any packet. When a packet is received, a check is made to determine its type in the INTERP_ACK state.
- *DISCARD*: The node discards the foreign frame (token, authorization or messages) and switches to the RECEIVE state.
- *DECODE_ACK*: The node updates its state with the ack received.
- *INTERPRET_ACK*: The node switches to the EVA_TKN, EVA_AUTH, EVA_MSG or EVA_FOREIGN state if the frame received is a token, an authorization, a message or an alien traffic frame, respectively.
- *EVALUATE_FOREIGN*: The node evaluates the alien message received.

The validation of protocols specified in terms of interacting finite state components can be useful in order to obtain the relevant parameters for the different operations involved in the timing model.

3.3.2 RT-WMP Processor Utilization

Let us consider the set X of all possible states of the RT-WMP's FSM. To respond to the reception of a frame, the FSM will go through a sequence of states $x_j \epsilon X$.

If we consider S to be the set of sequences of the FSM states we can define:

$$s_i = \{x_1, x_2, ..., x_n\}, \quad x_j \epsilon X, s_i \epsilon S. \tag{3.17}$$

For example, when a node receives a token, in order to forward it to another node, the protocol executes the sequence of states s_{tkn_fwd}:

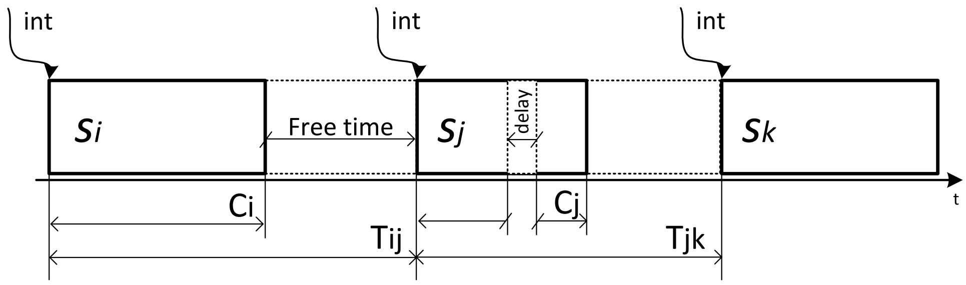


Figure 3.19: CPU time spent for the RT-WMP sequences.

$$
\begin{aligned}
s_{tkn\_fwd} &= RECEIVE \rightarrow DECODE\_RECEIVED \\
&\rightarrow INTERPRET\_RECEIVED \\
&\rightarrow EVALUATE\_TKN \rightarrow SEND\_TKN \\
&\rightarrow WAIT\_ACK
\end{aligned} \tag{3.18}
$$

When the sequence ends, the protocol leaves the CPU until the next event that provokes a new sequence to be run. The utilization factor of a sequence $U(S)$ is defined as the fraction of time spent by the CPU to execute a sequence taking into account the total amount of time in which the processor is free before executing another sequence. Consider Figure 3.19. The processor is occupied by the execution of the sequence s_i that has a computation time C_i and then is free until the execution of the subsequent sequence s_j.

Defining the period $T_{i,j}$ as the timespan between the triggering of two consecutive sequences s_i and s_j, the utilization factor $U(s_i)$ for the generic sequence s_i can be determined as:

$$U(s_i) = \frac{C_i}{T_{i,j}}, \tag{3.19}$$

In other words, the expression $U(s_i)$ is the percentage of the time that sequence s_i will occupy the processor as a response to each frame reception.

To reduce the processor occupation the protocol introduces a modulable delay before all send operations. It implies, as obvious, that the computation of the utilization factor of the sequences that include a transmission (like sequence s_j in the figure), must avoid to take into account this delay when measuring the execution time C_j.

Since we are interested in an upper bound in the processor utilization, we considered the worst-case i.e. the sequence that uses the most resources. Considering the maximum value obtained computing the $U(s_i)$ for each sequence i, we define the *worst-case achievable utilization* as:

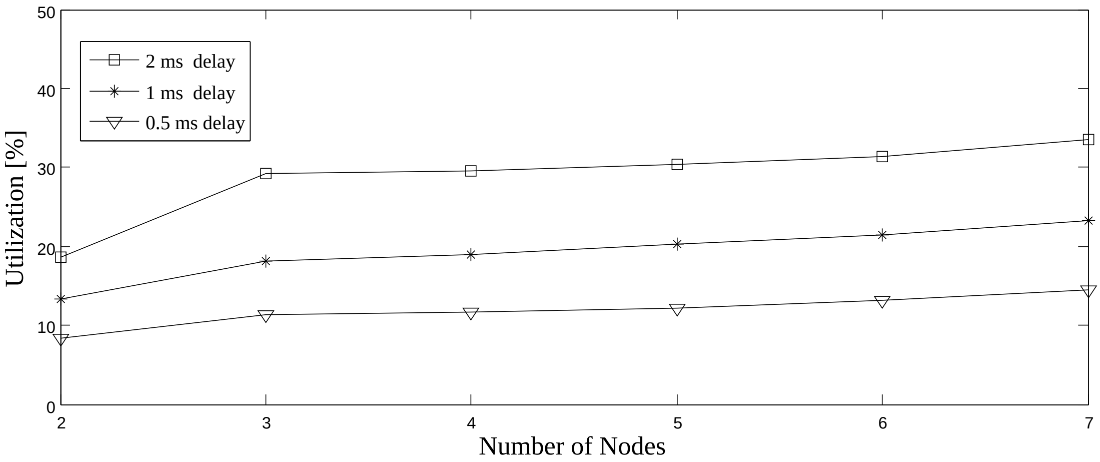


Figure 3.20: RT-WMP CPU utilization vs network size.

$$U = max\left\{\frac{C_i}{T_{i,j}}\right\}. \tag{3.20}$$

This will be considered as the maximum CPU utilization for the RT-WMP protocol.

3.3.3 Evaluation under MaRTE OS

Five nodes equipped with minimal embedded and dedicated hardware (100x160mm PcEngines ALIX3D3 board, battery powered), Atheros chipset-based wireless cards and running the MaRTE OS [Rivas 01] implementation of RT-WMP. Table 3.3 lists the parameter values used in the tests.

Utilization

Given that the protocol modifies medium access control, it is of interest to find out the protocol overhead added to the processor on which it is running.

In order to compute the utilization factor U, times have been measured as in equation 3.20.

As explained earlier, the protocol delay before transmission is a parameter introduced to control the use. We considered the impact of the network size on the utilization factor in a completely connected network. Measurements have been repeated for different delay values, 0.5, 1 and 2 $msec$, respectively. As can be seen in Figure 3.20, protocol delay positively affects the utilization because it leaves more free processing time. On the other hand, network size has a negative effect. This is because in a completely connected wireless network, a node receives all the frames

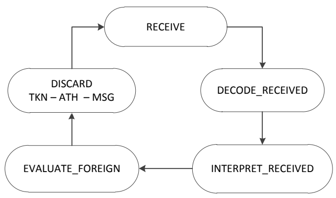
Sequence	**worst state**	**Utilization**
	RECEIVE	20.2%

Table 3.2: Main utilization result.

in the air, including those that are not for the node in question. Thus, the best situation is a two node network where no discard messages occur.

In fact, not completely connected networks are more frequent in real scenarios where packets have to travel on a multihop route to reach a node. The processor occupation can therefore be considered with reference to a value lower than the actual number of nodes in the network.

This is the case for example of a network of 7 nodes in a chain where, to achieve maximum coverage in length, a node can only sense the previous node and the following one. As far as the measurement is concerned, we should consider the value of 3 nodes.

The sequence with the maximum utilization is that involving the DISCARD state. This is mainly due to the frequency with which the sequence is repeated. In fact, in a completely connected network (as in the experiments) each node has to process each protocol frame in the channel, even those are not for the node in question and that will therefore be discarded. With respect to equation 3.20, $T_{i,j}$ represents the most influential factor for computing the utilization. Its low values mean that the utilization increases.

In addition, we have identified the execution of single state, i.e. the *RECEIVE*, that spends the time of the worst case sequence. This is due to the writing operation involved when a frame has been received. This is shown in Table 3.2 which considers the case of five nodes in a completely connected network that represents the worst case for this measurement.

3.3.4 Overhead and Blocking

One way of performing a characterization of a communication network is the estimation of the protocol Overhead and message Blocking.

In order to do this, let us first define the following main RT-WMP features:

- Number of nodes (N)

- Create a new token (CT): This operation is carried out to start a new PAP phase creating a token.
- Evaluate token (ET): This operation involves checking the token received and modifying it before the retransmission.
- Evaluate token and create Authorization (ETA): In the PAP phase, the last node checks the token, extracts the MPO node identity, and computes the path to reach the node that will be authorized. It then starts the ATP phase, sending the authorization.
- Evaluate Authorization (EA): During the ATP phase, each node on the path checks the authorization and forwards it to the next node.
- Evaluate Authorization and create Message (EAM): When the authorization reaches its destination, the node checks it and starts an MTP phase to send its highest priority message.
- Evaluate Message (EM): During the MTP phase, each node on the path checks the received message and forwards it to the next node.
- Evaluate Message Enqueue (EME): When the message reaches its destination, the node checks and enqueues it.
- Protocol Delay (PD): This is a delay introduced before any SEND operation.
- Header transmission (TH): This represents the time to send the header protocol bytes.
- Interrupt routine (ISR): This is the code executed by the interrupt server whenever a frame is received.

The duration of these periods is defined in the Appendix B.

With these attributes, we can estimate the packet *Overhead* and the *Max Blocking* for the RT-WMP, as in [Martínez 05].

- **Overhead**: It is the overhead caused by the protocol information that needs to be sent before each message. It is calculated as:

$$\begin{aligned} T_{overhead} &= \underbrace{CT}_{1} + \underbrace{(2N-4)\cdot ET}_{2} + \underbrace{ETA}_{3} + \\ &+ \underbrace{(N-2)\cdot EA}_{4} + \underbrace{EAM}_{5} + \underbrace{(N-2)\cdot EM}_{6} + \\ &+ \underbrace{TH}_{7} \end{aligned} \tag{3.21}$$

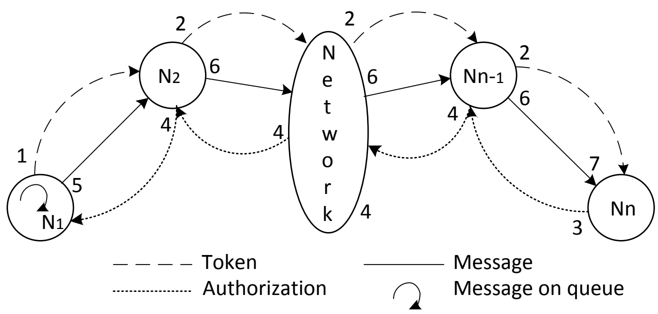


Figure 3.21: RT-WMP Overhead.

Figure 3.21 shows the worst case overhead case that can occur. In RT-WMP, this represents the time spent creating a new token and sending it (1), performing a complete circulation of the Token over the network (PAP phase can last up to $2N-4$ hops) (2), creating the authorization and sending it (3), and performing a complete circulation of the authorization to the N_1 (ATP phase can last $N-2$) (4). Node N_1 evaluates the authorization and prepares the message (5) that is to be forwarded (6). Finally, the penultimate node N_{n-1} evaluates the message and forwards it. We consider the cost of forwarding the message on the last hop, i.e. the protocol header message (7).

- **Non Preemptive Blocking**: The blocking is caused by the non-preemptibility of message packets.

  Priority inversion occurs when a higher priority message is blocked by lower priority messages. If the lower priority message gains access first and then the higher priority message requests access to be sent, this is blocked until the lower priority message completes its loop. Thus, blocking is a form of priority inversion where a higher priority message must wait for the processing of a lower priority message.

  In RT-WMP, blocking represents a complete token and the authorization phase plus the blocking effect caused by the transmission of a lower priority packet. This is calculated as:

$$\begin{aligned} B_{NP} &= \underbrace{(2N-5)\cdot ET}_{2} + \underbrace{ETA}_{3} + \underbrace{(N-2)\cdot EA}_{4} + \\ &+ \underbrace{EAM}_{5} + \underbrace{(N-2)\cdot EM}_{6} + \underbrace{EME}_{7} + \\ &+ \underbrace{CT}_{8} + \underbrace{(2N-4)\cdot ET}_{9} + \underbrace{EAM}_{10} \end{aligned} \tag{3.22}$$

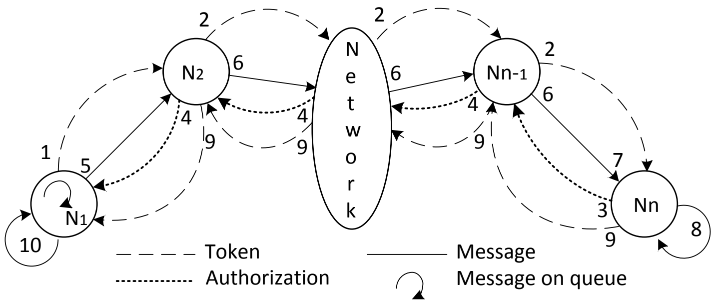


Figure 3.22: RT-WMP Max Blocking.

In order to understand the previous equation, see figure 3.22. Node N_1 has a message to send in its transmission queue. It actualizes the token received with the priority information of this message and forwards the token (1). At the same time, node N_1 receives from a thread a most priority message to transmit throughout the network. This message should be transmitted but it will be subject to blocking because the priority information of the previous message has already been included in the token. The token reaches the other nodes (with up to $2N-5$ hops) (2). The last node to receive the token, N_n, evaluates the token, computes the path to the node which will be authorized and prepares the authorization (3). It then initiates the authorization phase that will end at the first node (4). N_1 is now authorized to transmit the (previous) message to the destination (this phase could last up to $N-2$) (6).

The destination node (N_n, in the worst case) starts a new PAP phase, creating a new token (8) that will travel through all the nodes (9). At the end, node N_1 can authorize itself (10) to send the most priority message that has been blocked.

3.3.5 Message Response Time

Holistic schedulability analysis has been proposed for data in distributed Hard real-time multitasking systems with static priority preemptive scheduling, as in [Tindell 94]. This analysis can be applied to the RT-WMP model.

For a given message i, the *worst case response time* R is the message access time to the network t_{Ai} and the time it takes the message to be delivered to the destination node T_i:

$$R_i = t_{Ai} + T_i, \tag{3.23}$$

T_i is the time taken by the protocol to deliver the messages i to the destination, that is the RT-WMP protocol cycle, as explained earlier (see eq. 3.8).

	Parameter	**Values**
Scenario	Channel rate	6 Mbps
	Number of nodes	up to 7
Data	Real-Time pkt	1024 Byte
Constraint	Protocol Delay	0.5 - 1 - 2 ms

Table 3.3: Communication parameters used in the experiment

The message access time to the network t_{Ai}, or the time spent in the queue, can be considered in terms of the monotonic scheduling policy. Queueing delay is composed of the longest time that any lower priority message can occupy the network, i.e. the blocking time B_{NP}, and the longest time that all higher priority messages can queue and occupy the network before the message m is finally transmitted. The latter time is defined as *interference* [Audsley 93], i.e. the number of cycles it must wait until being sent because there are enqueued messages of higher priority.

So, it is possible to define t_{Ai} as:

$$t_{Ai} = B_{NP} + I$$

The interference time I for a set H_p of all messages of higher priority than a given message i over an interval of duration t_i is defined as:

$$I = \sum_{j \epsilon H_p} \left\lceil \frac{t_i}{P_j} \right\rceil T_j,$$

where P_j is the period of the j message. The t_i/P_j factor represents the number of times messages of higher priority arrives during t_i.

Considering the time elapsed as the message response time, $t_i \equiv R_i$, the equation 3.23 can be rewritten as:

$$R_i = B_{NP} + \sum_{j \epsilon H_p} \left\lceil \frac{R_i}{P_j} \right\rceil T_j + T_i, \tag{3.24}$$

The interference depends on R_i itself, thus a recurrence relation can be formed to obtain the final value of the response delay. Or, to simplify, we can consider the duration t_i as the blocking time. In fact, every message that arrives before $T_{Blocking}$, including the higher priority messages, have to wait in the queue.

3.4 Conclusion

We have presented a detailed evaluation of all the RT-WMP characteristics presented in the previous chapter.

The theoretical analysis has shown how each RT-WMP event/phase has a bounded and known duration and how the protocol offers a bandwidth similar to or better than that offered by the 802.11 plain protocol in worst-case multi-hop situations. It is comparable to the 802.11 protocol in relatively small and completely connected networks, while it offers similar or better performance with RTS/CTS mechanisms. The extensive real tests have demonstrated that the protocol is capable of offering a good worst-case real-time communication bandwidth for different network sizes, respecting priority delivery and fairness and with bounded worst-case end-to-end delay.

The results are interesting especially considering the worst-case situation which, as explained, must be taken into account at the planning stage. Notice the results do not take into account any routing protocol that must be used on top of the plain 802.11 which would add additional overhead.

Moreover, a comparison between RT-WMP and the general purpose protocol OLSR is offered both in terms of worst situation bandwidth and mobility capabilities. This testbed comparison has shown how general purpose routing protocols can not easily be used for time-sensitive mobile applications due to the unpredictability of the end-to-end delay, to the absence of priority support and to the poor performance in terms of mobility management.

Finally, we have shown that the protocol is analyzable. An in-depth protocol analysis has been presented, representing a contribution to the possibility of using RT-WMP as a communication framework in distributed real time systems.

The evaluation presented in this chapter is a totally original contribution of this thesis which provides a global vision of the main features of the RT-WMP.

Chapter 4

RT-WMP Quality of Service Extension

The widespread use of wireless devices in applications involving humans confirms the need for supporting multimedia traffic. As a result, researchers have proposed several methods to offer some kind of Quality of Service (QoS) on MANETs.

In applications involving real-time systems, such as robotics, it is of interest to consider QoS requirements together with real-time requirements. For example, in certain fields of application such as emergencies, rescue situations, battlefields or hostile environments, the possibility of establishing some type of multimedia communication could be useful. An example might be audio streaming amongst rescuers and victims to obtain information about the status of people involved in an emergency. In some situations, visual information such as photo or video streaming could be effective for easing access to disaster zones.

However, both flows of information, real-time for robot control and QoS for multimedia traffic, have quite strict time requirements and, at first sight, could be thought of as real-time flows. It might therefore be considered a good idea to take these flows into account at the planning stage and treat them as normal real-time flows.

On the one hand these flows are quite bandwidth consuming and in some specific situations they might not be possible o achieve (depending on the saturation of the real-time bandwidth) while, on the other hand, not all the frames necessarily have to be delivered. As an example, the iLBC [Andersen 02] or speex [RFC5574 09] audio codecs guarantee, at low bit rate, a MOS (Mean Opinion Square) greater than 3.3 and 2.5, respectively, with a packet delivery ratio (PDR) of about 95%.

In this chapter we propose a novel solution to incorporate multimedia traffic in a real-time wireless communication network without jeopardizing the hard real-time traffic. This idea has been implemented and analyzed as an extension of the RT-WMP protocol, defined in the previous chapter. The rationale is to take advantage of the bandwidth left free by the protocol when it is not working in the worst-case situation and use it to send QoS frames to allow audio and video streaming flows.

This contribution has been developed within the framework of the NERO Spanish National Project and the European Commission URUS project. The results of this work were presented at the First International Conference on Ad-Hoc Networks held from September 23 to 25, 2009 in Niagara Falls, Ontario, Canada and published in “Ad-Hoc Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering” with the title “QoS over Real-Time Wireless Multi-hop Protocol” [Sicignano 10a].

4.1 Related Work

The growing interest in offering multimedia on wireless networks has led to a breakthrough in studies obout offering Quality of Service over MANET. 802.11 based networks present several technical barriers that need to be overcome in order to offer a reliable solution to this problem. On one hand the per-packet transmission overhead, that includes per-packet header bits, link-layer acknowledgment, back-off delay to avoid contention, retransmission due to channel interference and inter-frame spacing for synchronization. It cause a gap between theory and practice performances in the packet’s transmission. A second technical barrier is lack of an specific QoS support. Despite ITU-T recommendation, native 802.11 networks have neither a precise control over the transmission timings of multimedia frames (due to collision and random back-off) nor a traffic priorization service. Consequently, no prioritized traffic may consume a large proportion of the network capacity, at the expense of time-sensitive multimedia traffic.

Protocols like 802.11e [Mangold 02] [IEEE 05], for example, try to introduce a certain degree of determinism at the MAC layer prioritizing traffic as a function of its type and class. Other researchers have proposed interesting solutions for offering QoS guarantees over multi-hop networks modifying this protocol. This is the case of [Hamidian 07] where the authors add a QoS mechanism to the enhanced distributed channel access (EDCA) scheme to allow a resource reservation or [Reddy 07] where packets are prioritized using a combination of the laxity of the packet and the number of hops to the destination node to give higher priority to the packets that have to traverse many hops.

Other solution are based on a token-passing scheme. In [Ergen 03] the potential of achieving higher channel utilization using a token scheme compared to CSMA based schemes is shown. More recently, in [Wang 07], the advantage of a token-passing scheme over contention based and centralized polling schemes to provide guaranteed priority for different traffic classes in WLAN has been analyzed. A similar analysis is conduced in [Zhang 08] which shows how a token ring scheme applied in vehicular ad-hoc networks can outperform IEEE 802.11 DCF in terms of average throughput. The wireless dynamic token protocol (WDTP)[Zhai 06] modifies the method to control the token transfer scheme of the WTRP. All nodes are clustered into subnets and the nodes of a subnet share a channel. This improves the adaptability to the network topology but the number of used channels increases. Some proposals are based on hybrid MAC Token CDMA policing mechanisms. Taheri and Scaglione's [Taheri 02] proposal is based on a ring network where each token corresponds to a physical CDMA subchannel which is guaranteed to have a certain average rate and satisfies a probability of error bound by identifying two classes of service to give prority to QoS traffic.

All these solutions, despite offering some degree of timing guarantees, have a quite different target than the solution proposed in this chapter, since the only objective is to offer QoS support without considering the real-time requirements. Currently, to the best of our knowledge, there is no protocol that allows the simultaneous transportation of real-time and QoS traffic.

4.2 Overview

In real-time systems, planning must always be carried out considering the worst possible scenario. However, worst-case loops are unlikely to happen in practice and even with unfavorable network topologies they occur only in a small percentage of loops. The rationale behind this proposal is, therefore, to take advantage of the time considered at planning time but not actually used in the majority of situations. From the communication point of view in a distributed real-time system, this can be translated to the time interval between a concrete end-to-end delivery delay and the worstcase delivery delay. In other words, we are taking advantage of the fact that the worst case will take place in very few situations, using the time left to transport QoS data flows or best effort traffic.

4.2.1 Worst-case in RT-WMP

RT-WMP protocol phases have a bounded duration (see section 3.1.1). As described by equation 3.3, the worst-case end-to-end delivery delay can be expressed as:

$$t_{ete}(wc) = 2 \cdot t_{loop}(wc) \tag{4.1}$$

This value depends, in turn, on the network topology and on the position of the source and destination of any specific message. Worst-case loops are unlikely to happen in practice and even with unfavorable network topologies they occur only in a small percentage of loops. In other words, in the majority of cases the RT-WMP closes its loops in a time shorter than the worst-case one and in some cases (if the real-time traffic bandwidth usage is below one-hundred percent) the loop consists of the PAP only. The idea, therefore, consists of using, in any loop, the time slot between the real loop-duration and the worst case loop duration to send QoS information. In other words, we are forcing the protocol, when one or more QoS flows are present, to operate in the worst-case situation taking advantage

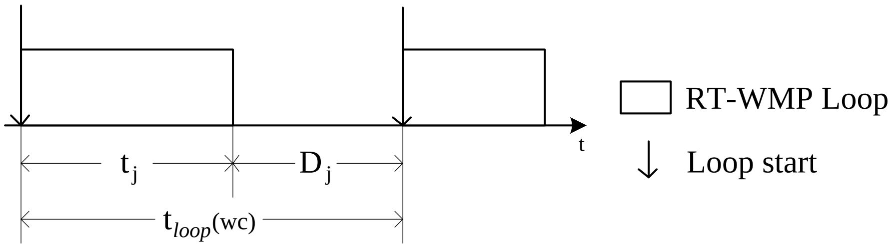


Figure 4.1: Time intervals used by the QoS Extension.

of the fact that it will take place in very few situations. So, real-time characteristic of the protocol is guaranteed.

This scheme does not worsen, by design, the worst-case end-to-end so can be used in any real-time network to add QoS capabilities maintaining the same worst-case performances.

4.2.2 Available Time

The available time in any loop depends on several factors such as the relative position of source and destination, the network topology and so on. The duration of the real RT-WMP loop t_j is *less than or equal* to the worst-case loop $t_{loop}(wc)$. Figure 4.1 illustrates the situation. The available time D_j can be expressed as:

$$D_j = t_{loop}(wc) - t_j \tag{4.2}$$

While the minimum value of D_j is zero, the maximum corresponds to the situation in which the RT-WMP loop is only constituted by the PAP. In this case $D_j = t_{loop}(wc) - T_{PAP}$.

4.2.3 QoS Extension Operations

To each node has been added a QoS transmission and reception queue (QTQ and QRQ respectively). Each QoS message has a deadline that is fixed by the application and that represents the time during the which the message is valid.

This QoS extension, has three phases: an arbitration phase, a QoS Authorization Phase (QAP) and a QoS Message Phase (QMP) that can be repeated one after the other for a limited amount of time. The arbitration phase is carried out during the PAP while the QAP and QMP, are added to the basic protocol.

In the arbitration phase *all* the nodes which have a QoS message waiting in the QTQ compete to gain the right to send it (during the PAP the token reaches all the nodes). One or more messages can be selected for transmission depending on their deadline and on the distance between the source and the destination nodes, as will be explained below. The address of the nodes owner of these messages are stored in the header of the frames. The first QAP starts when the standard MTP ends (or after the PAP if there is no real-time message to be sent). The node which ends the MTP (or the PAP), instead of restarting the successive PAP, sends an authorization to the owner of the first selected message (indicated in the header), using the same scheme used by the RT-WMP. The latter, then starts the QMP and sends the QoS message to the destination node that pushes the message into its QRQ. Successively, if the header specifies that there are other messages to be sent, it prepares an authorization and starts another QAP during which the message reaches the node owner of the selected message. This, in turn, sends its message during a further QMP and so on. As has been stated, the QAP and QMP are been repeated one after the other for a limited (and configurable) number of times, but in any case they stop when the worst-case loop time is reached. This behavior is obtained by loading a field of the header with the duration, expressed in milliseconds, of the worst-case loop and subtracting, in any frame-pass, the time spent on this action. When this value is lower than the time needed to execute the next frame-pass, the QAP or QMP ends and a normal PAP restarts. If the PAP has to restart during a QMP, the transported message is stored in the QTQ of an intermediate node to be able to compete for selection again in the successive PAP.

The QoS extension implements eight flow priority classes where class zero corresponds to best-effort not-QoS traffic. Flows are served following their priority level. Audio flows, for example, usually have priority over ideo flows since audio information is more delay sensitive. The introduction of a flow in the protocol is regulated by the Flow Admision Control (FAC) that allows or denies access, taking into account the priority of the requesting flow and the available bandwidth estimatedby analysing the differece between the worst-case and the real loops durations within a certain time-window.

4.3 The RT-WMP QoS Extension Details

In Real-Time distributed systems, bounded end-to-end delay and priority support are required for scheduling and time constraint guarantees. Since the plain RT-WMP is a real-time protocol, each event/phase protocol has a bounded and known duration even in the presence of the majority of errors. Loops have, for example, an upper bound on their duration that can be easily calculated and that is used as a base to calculate the loop remaining time, as will be explained with more details below.

4.3.1 Frame Header Modification

Figure 4.2 shows the RT-WMP frame with the fields that support the QoS extension. The *qos_rem* field is a 2 byte field that is filled, at the beginning of any loop, with the duration, expressed in milliseconds of the worst-case RT-WMP loop. The

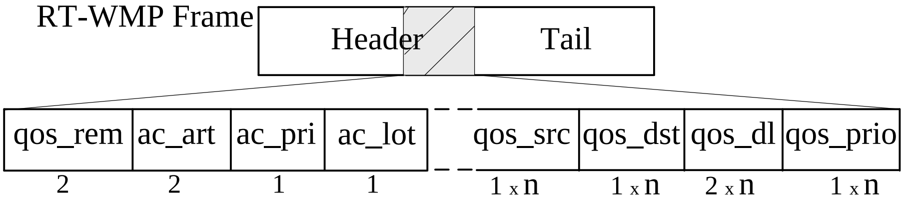


Figure 4.2: Frame for the RT-WMP with QoS extension.

ac_loop_id, *ac_pri*, and *ac_lot* are service fields used by the access control system to estimate the available QoS bandwidth. The next fields are used to identify the selected messages. All of them are (compile-time) configurable size vectors. Their size is application and network-size dependent and represents the maximum number of QoS messages that can be selected (and potentially delivered) in any loop. The *qos_dl* (2 bytes per message) contains the actual deadline of the packets (relative deadline to the actual moment) while the *qos_src* and *qos_dst* (1 byte per message) specify their source and destination. These last three fields are used to calculate the dynamic priority of the message that depends on the deadline and the distance between the source and destination of a message. The last *qos_pri* field (1 byte per message) carries the priority class of the selected message.

4.3.2 Phases of the Protocol

In this section a detailed description of the different phases of the protocol is presented including some implementation issues than condition the development of the protocol.

The Message Selection Phase

The first phase of the protocol takes place simultaneously with the PAP of the basic RT-WMP. In fact, in this phase the QoS extension does not alter the operations of the basic protocol (tokens are exchanged in the usual way). In this phase, the QoS messages to be transmitted in the successive phases are selected. In each node the QTQ contains all the QoS messages ordered by priority (see sec. 4.3.3).

The node that starts the PAP analyses the QTQ. Above all, it discards the expired messages. It then obtains the class flow, the deadline and the destination of the n most priority messages (n being the maximum number of QoS messages that can be delivered in any loop) and fills the correspondent fields of the token header. Moreover it calculates the worst-case loop duration and fills the field *qos_rem* of the header with this value expressed in milliseconds. Successively the basic protocol is responsible for sending the token to another node. The node that receives the token processes the basic part of the token as usual. It then actualizes the values of *qos_rem* and the *qos_dl* subtracting the time spent in the last token-pass. It successively calculates the new priority for the messages referenced by the token. This step is necessary because the change in the deadline implies a change in priority. It then again discards expired messages and compares the n most priority messages in the QTQ with those carried by the token. If figures out that owns one or more priority messages, and replaces the less priority with its own updating of the *qos_dl*, *qos_src* and the *qos_dst* fields. In the same way, the process is repeated up to the moment in which the last node of the network is reached. At this moment the node starts the ATP and the MTP (if real-time messages have been selected to be sent). In these two phases, there is no participation of the QoS extension except for the fact that the *qos_dl* field is decreased by the quantity corresponding to the time spent in any frame pass.

The QoS Authorization Phase

This phase starts after the conclusion of the MTP (if any) or the PAP or even after a QMP. The node that starts the QAP prepares an authorization as in the basic protocol (see [Tardioli 07]), fills the *aut_src* with its address and *aut_dest* with the first element of the *qos_dst* vector, shifts by one the position of the *qos_dst*, *qos_dl*, *qos_pri* and *qos_src* vector elements (*qos_dl[0]=qos_dl[1], qos_src[0]=qos_src[1], etc.*) and sends the frame.

The authorization is propagated using the same routing algorithm of the basic protocol (Dijkstra based algorithm) until it reaches the destination. In any hop, however, the *qos_dl* and *qos_rem* fields are actualized subtracting the duration of any frame-pass. If at some moment the *qos_rem* field reaches a zero value (or a value that does not allow a further frame-pass), the QAP is immediately aborted and another PAP is started.

The QoS Message Phase

When a node receives a QoS Authorization, the QMP starts. It pops the most priority message from the QTQ and creates a new message frame placing data in the *message* field. It fills the *src* and *dest* fields with its address and with the destination address and calculates the path to the destination. Then it sends the message to the first member of the path as in the RT-WMP basic protocol. When the latter receives the message, it checks the *msg_dest* field. If it is not the destination node (i.e. if it is an intermediate node), it verifies if there is enough remaining time to forward the message to the next node of the path (i.e. the value of *qos_rem* is at least greater than the time needed for one message-hop). If this is the case, the node repeats the computation of the path and routes the message to the next member of the path, leaving the *dest* field unchanged. Otherwise, it pushes the message into the transmission QoS queue and starts a new PAP. In this case the message will compete to be selected for transmission again in the next PAP. If the message reaches the destination in a single loop, there is the chance of sending another QoS message. When the node receives the QoS message, it pushes it into the QRQ. It then looks at the *qos_rem* field. If it is assured that there is enough time to authorize another node and to allow at least one message-hop, it starts another QAP that, in turn, will cause another QMP and so on.

4.3.3 Message Priority Policy

Packet Deadline

Timing guarantees can be considered as a fundamental feature for MANETs able to support QoS applications. Applications such as voice communication, video-on-demand, video conferencing, and radio broadcasting require that the end-to-end delay be less than a certain value. Thus, each packet has to reach the destination within the specified deadline, after which it becomes useless.

In a single-hop network the queueing delay is not too large. However, in the multi-hop scenario, the source and destination may be several hops away, and packets need to be forwarded by the intermediate nodes. As a result, delays can become quite large, especially due to the presence on the networks of packets with highter priority thereby making audio and video transmissions infeasible.

In order to grant a good QoS level, each message has to be delivered before its deadline. Delay bounded service allows the protocol to know whether it is able to meet the deadlines or not. Any QoS packet has an associated deadline by which it must be delivered. If this is not possible, the packet must be discarded. Indeed, when deadline is met before the destination node, packet is useless for the audio/video and occupy network resources unnecessarily. This deadline value is only needed until the packet is either successfully transmitted or discarded.

The mechanism to label and update the deadline on every QoS message is quite simple. Messages are labelled with their maximum admitted deadline, depending on the nature of message. Deadline values are usually 150 ms for voice and 400 ms for video traffic that correspond to maximum end-to-end delays admitted for multimedia traffic [Vlaovic 01]. When this parameter reaches the zero value, the message expires. So, during multi-hop transmission, this value has to be properly updated. Every node over the source-destination path updates packet deadlines taking into account the elapsed time and the transmission time of one-hop.

Packet Scheduling

The QoS extension implements a packet scheduler that assigns a dynamic priority to a packet taking into account the flow class, the deadline and the number of hops left to the destination, in this order. Above all, the scheduler sorts the packets according to their class flow. Messages in the same flow-class are sorted using the *laxity* that is a parameter that combines the deadline and the number of hops left to the destination as $laxity = deadline/hopleft$.

Instead of transmitting packets in the FIFO order (as in the case of 802.11e) or EDF order, we prioritize the packets with respect to the laxity. In fact, in 802.11e for example, a packet whose destination is one hop away has the same possibility of capturing the channel as a packet whose destination is several hops away. So, locally it does not take into consideration the number of hops a packet has to cross. However, the laxity gives us an estimate of how much delay the packet can tolerate at each hop. Hence, the packet with the lowest value of laxity is given the highest priority. If two packets have the same lowest value of laxity, we resolve the conflict by sending the packet which has more hops to travel. If the laxity value becomes zero, the packet is discarded since it is useless at the destination.

4.4 Flow Admission Control

In Ad-hoc networks, distributing shared network resource between competing users has become one of the fundamental challenges. The limited bandwidth capacity makes it difficult to guarantee the QoS requirements in the presence of many flows. Therefore, it is necessary to have a good estimation of the bandwidth required by a flow. The more exact this estimation is, the more efficient the admission control would be. FAC is considered as an important component for the provision of QoS parameters. The aim of FAC is to limit the amount of traffic admitted into a network so that the QoS of the existing flows will not be degraded.

Actually most of work to provide a FAC mechanism in MANETs is done for a MAC layer. Most of these are provided by APs and they are not suitable in a purely MANET, without infrastructure. Reference [Yan 08] presents an distribuited admission control mechanism based on finding a avalilable path during the routing establishment. In [Hung-Yu 06] the authors propose an interesting model-based approach that work trying to maintain the QoS metric of existing flows while maximizing the number of admitted calls. That scheme uses the nodes interference in order to evaluate the state of channel ocupancy. Another model-based approach is presented in [Zhang 06], where a distributed time allocation allows to balance the bandwidth amongst flows with a low computation complexity. In [Canales 07], authors propose a mechanism to evaluate the QoS demand based working on a routing algotithm and MAC layer to ajust the decision taking into account the scenario variabilty. The authors in [Yigitbasi 08] present a synchronous bandwith allocation scheme based on timed token protocol in a centralized control plane and limited to a token ring network.

4.4.1 Overview

The available bandwidth for QoS flows is limited and depends on different factors such as real-time flow saturation, network topology and so on. Thus, it is important to control the admission of new QoS flows in a real-time network since if the available bandwidth is not enough, it is possible to jeopardize the correctness of the whole set of flows. As an example, consider the situation in which in the network there already exists a 15Kbps flow and the global available bandwidth for QoS flow is about 20 Kbps. If we try to introduce another 15 Kbps flow of the same class, the system will distribute the available bandwidth between the two flows lowering the rate of both to 10 Kbps discarding the messages that cannot be delivered within the deadline. It would not be enough for a correct streaming and both flows would be useless. FAC estimates and manages the available bandwidth. The idea is to compute if there exist enough bandwidth for a given new flow. The admission control works in accordance with the flow *class*.

4.4.2 Available Resource Estimation

To estimate the available bandwidth for new QoS flows, the network is observed during a time window that contains several RT-WMP loops. We call this sliding window the *Available Bandwidth Estimation Interval* (ABEI). The width of the ABEI is configurable and a good choice is usually related to the hyperperiod of the underlying real-time distributed system.

Over an ABEI the *Global Remaining Time* (GRT) is calculated as:

$$GRT = \sum_{j:loop_j \epsilon ABEI} D_j. \tag{4.3}$$

The GRT represents the sum of all the remaining time D_j that is included in the ABEI. In other words, the GRT is a measure of the available time for QoS flows. Any QoS flow occupies a portion of this global available time. We call the sum of all the occupied portions Global Used Remaining Time (GURT) that can be expressed as:

$$GURT = \sum_{j:loop_j \epsilon ABEI, k \epsilon [0..7]} td_j(k) \tag{4.4}$$

$td_j(k)$ being the time consumed by a k class flow in a loop j (see Figure4.3). In a similar way it is possible to define the Global Available Remaining Time (GART) as $GART = GRT - GURT$.

The GART represents the time still available subtracting the time occupied by already-active QoS flows. However, this access control scheme relies on flow classes, that is, higher priority flows can expel lower priority ones. In the light of this, the GART can be considered as the available time for the least-priority flow in the system at any moment. The available time for a given class flow is instead called the Available Remaining Time (ART). It can be expressed as:

$$ART(c) = GRT - \sum_{j:loop_j \epsilon ABEI, k \geq c} td_j(k) \tag{4.5}$$

c being the class of the flow that is requesting access.

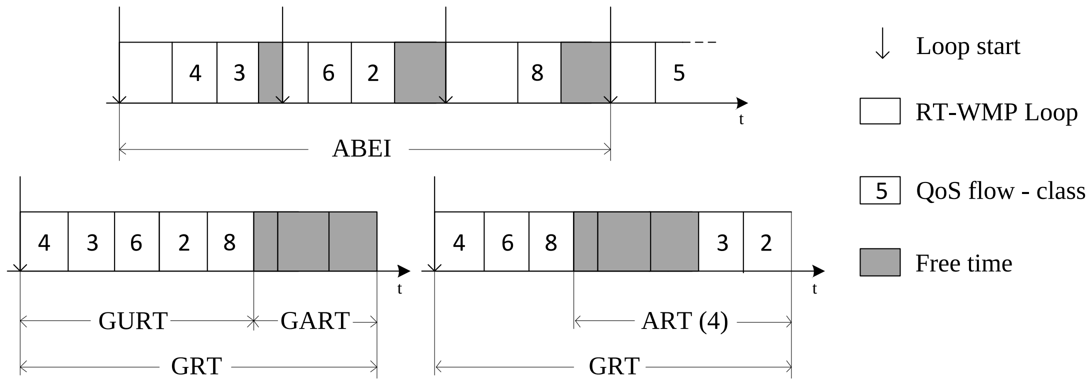


Figure 4.3: Resource estimation mechanism.

If a flow requests access to the system, the FAC calculates the ART for the class flow of the flow requesting access and estimates (using a heuristic) whether there is enough bandwidth to allow the access.

Principle of Operations.

When a node closes a PAP, it stores in a local vector the value of *qos_rem* together with a timestamp. Next, it fills the *ac_lot* field with the value of the *qos_rem* field. Successively, when a QoS Message is delivered, if k is the class flow of the message, the receiver computes the time spent to deliver the last message with the formula:

$$td(k) = ac\_lot - qos\_rem \tag{4.6}$$

The node stores td in a local vector together with the class of the message just received. Then it actualizes the value of the *ac_lot* with the present value of *qos_rem* and continues the operations with another QAP or a new PAP. The process is repeated in any loop and the nodes accumulate, but in a distributed fashion, all the information about message delivery times and remaining times. In fact, none of the nodes has a global view of the available time in the network. However, the sum of all the elements of the first vector of all the nodes represents the GRT and the sum of all the elements of the second vector represents just the time consumed by all the active flows in a specific moment (i.e. the GART).

When a node needs to add a new flow into the network, it requests that it specify the class of the new flow in the *ac_pri* field (that normally contains a negative value). In the successive PAP, all the nodes analyse their vectors with respect to the values stored in the ABEI window. Specifically they sum all the values of the first vector whose timestamp is contained in the ABEI and subtract all the values of the second vectors whose timestamp is contained in the ABEI *and* class is greater or equal to the one requesting the flow. The result of this computation is added to the values of the *ac_art* field (that normally contains a

	Parameter	Values
Scenario	Channel rate	1 Mbps
	Number of nodes	6
Data	Real-Time pkt	128-256-512 Byte
	QoS rate per flow	15 Kbps
Constraints	Deadline	150 ms
	Queues size	50 pkts

Table 4.1: Parameters used in the real tests.

null value). When the token has reached all the nodes, the *qos_art* field contains the Available Remaining Time (ART) of the given class flow.

Figure 4.3 shows the rationale behind the procedure. The global time left free by the protocol in an estimation interval is consumed by the time spent to deliver QoS messages of any class. However, when a message requires access, only higher classes messages are considered in order to calculate the ART for this class flow. When in the next PAP the token again reaches the requesting node, it analyses the value contained in *ac_art*. Using a simple heuristic, the node decides if the requesting flow is admissible. If this is the case, it allows the application to begin the new stream.

4.5 Evaluation

The aim of our experiments is to examine the impact of the proposed extension on the RT-WMP protocol. Several real tests have been made using an implementation of RT-WMP executed over the MaRTE OS [Rivas 01] real-time operating system. A total of six nodes equipped with Intel Pentium IV CPU at 2.5GHz, 2GB RAM and Ralink RT61 chipset-based wireless cards have been used. To evaluate the correctness, the performance and the behavior of the protocol extension, we have performed some real experiments. Table 4.1 lists the parameter values used in the tests.

4.5.1 Available Time

Figure 4.4 shows the result. In figure 4.4.a we can observe that the connected topology leaves a mean of Dj = 61:75 ms available for QoS traffic considering a worst-case loop of about tloop(wc) = 78 ms, that is about 80time. Both the string and the star topology are quite demanding leaving a mean of about Dj = 30 ms (38).

The proposed extension uses the available time $D_j = t_{loop}(wc) - t_j$ to transmit the QoS traffic. An real experiment was carried out to evaluate the dependency of

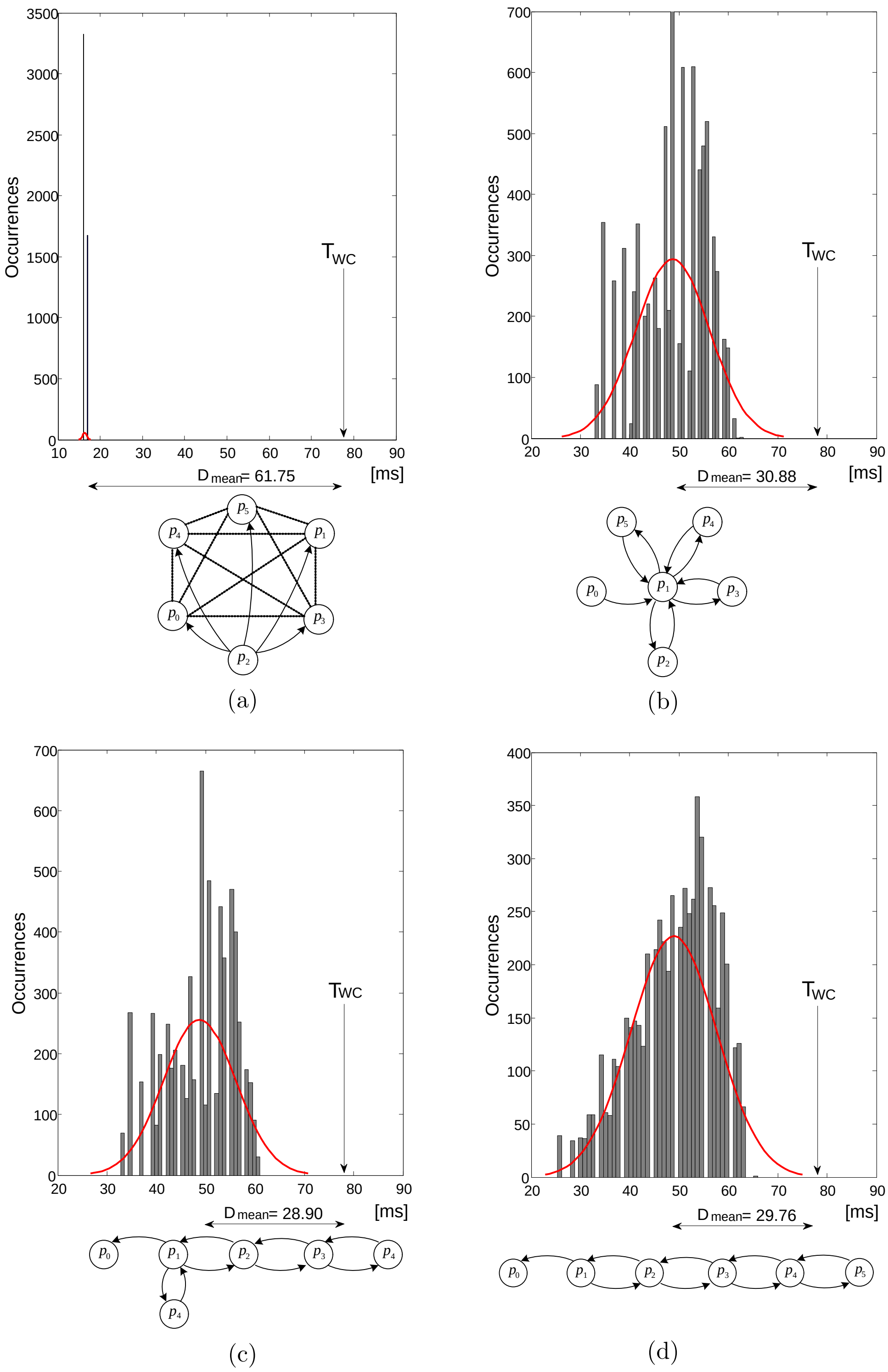


Figure 4.4: Time spent for the RT-WMP in real test compared to worst case for different topologies.

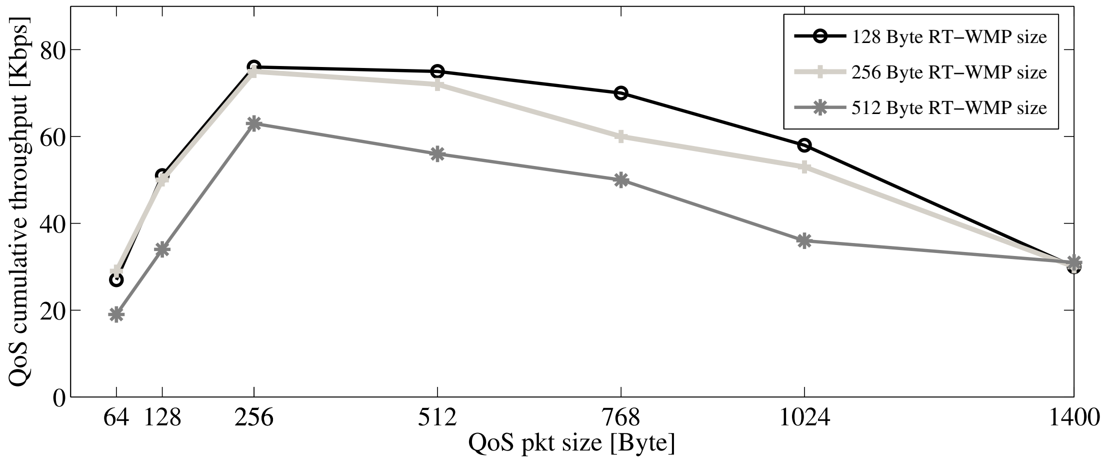


Figure 4.5: QoS Cumulative Throughput vs. protocol packet size.

the available time for QoS traffic on the network topology simulating four different topologies: a completely connected network, a "gun" network a star network, a "gun" network and a chain network. In the last three configurations, worst-case loops can occur while in the first of them all are best-case loops. The protocol has been forced to work with saturated real-time traffic (i.e, there is a real-time message in each RT-WMP loop). Figure 4.4 shows the time spent (t_j) by RT-WMP in the trasmisison of the real-time messages versus the worst case loop time ($t_{loop}(wc)$).

The measure allows us to evaluate the actual time D_j that RT-WMP can make available to the QoS extension when the PAP, APT and MTP phases are finalized. We can observe that the connected topology leaves a mean of $Dj = 61,75ms$ available for QoS traffic considering a worst-case loop of about $tloop(wc) = 78ms$, that is about 80% of the time. The other topology are quite demanding leaving a mean of about $Dj = 30ms(38\%)$.

4.5.2 RT-WMP Traffic Impact

QoS performance depends on real-time traffic. The aim of the second experiment was to consider the impact of the real-time and QoS message size on QoS traffic.

Figure 4.5 shows the cumulative QoS throughput of 5 traffic flows (of 15 Kbps rate each one) in the presence of RT-WMP traffic generated to saturate the network resources versus the QoS packet size. The measurements were repeated for different real-time packet sizes, 128, 256 and 512 bytes respectively. The better throughput was obtained by a RT-WMP packet size of 128 bytes with QoS flow packet sizes of 256 bytes. The shape of the graphic is due to the fact that small dimension packets increase the relative weight of authorization phases with negative consequences for efficiency. On the other hand, big packets (generated at the same rate) increase losses due to the being deadline.

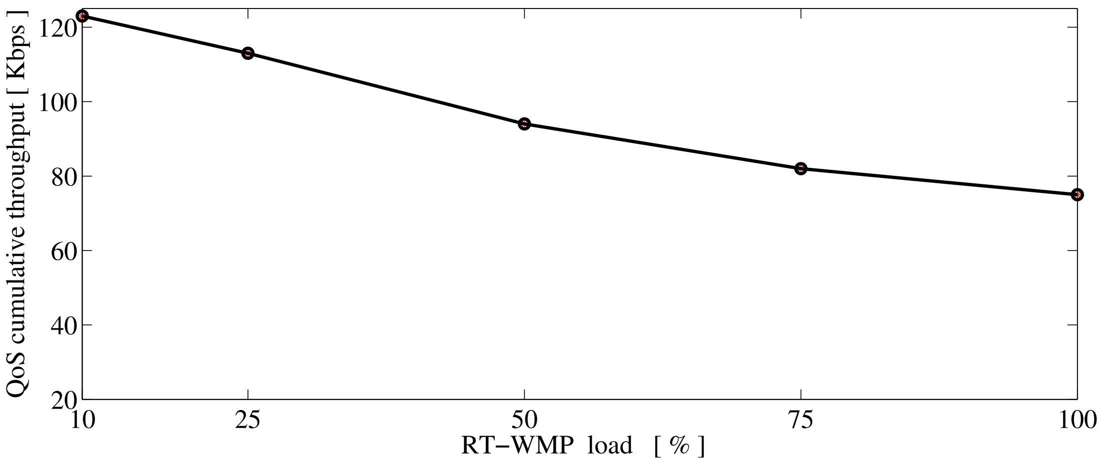


Figure 4.6: QoS Cumulative Throughput vs. RT-WMP load percentile.

Figure 4.6 shows the effect of the RT-WMP load on the QoS traffic. 100% means that all RT-WMP loops have a real-time message to send in the MTP phase. Obviously, a lower RT-WMP load benefits the QoS throughput.

4.5.3 Fairness

For several reasons (partially connected topology, channel access method and hidden terminals), the contention among stations in an ad-hoc network is not homogeneous. Some nodes can suffer severe throughput degradation especially when the load is high. This is known as the *fairness problem* and IEEE 802.11 does not resolve it [Wang 01]. The RT-WMP QoS extension, working over 802.11, guarantees fairness amongst nodes. So we verified that sender nodes achieve very similar instantaneous throughput. In other words, throughput of same class flows shows very small deviations. This is showed in Figure 4.7.

4.5.4 End-to-end Delay

Delay can degrade the audio and video applications. For such applications end-to-end delays have to be limited.
We have evaluated end-to-end from the point of view of flow class. Figure 4.8 shows end-to-end delay values obtained over 5 QoS flows. Figure 4.8.a compares delays of different class flows. As can be seen, delays turn out to be limited and, in the case of same class flows (Figure 4.8.b), they suffer a very small variation. The system thus becomes more responsive to the high priority traffic granting similar delivery times to same class flows.

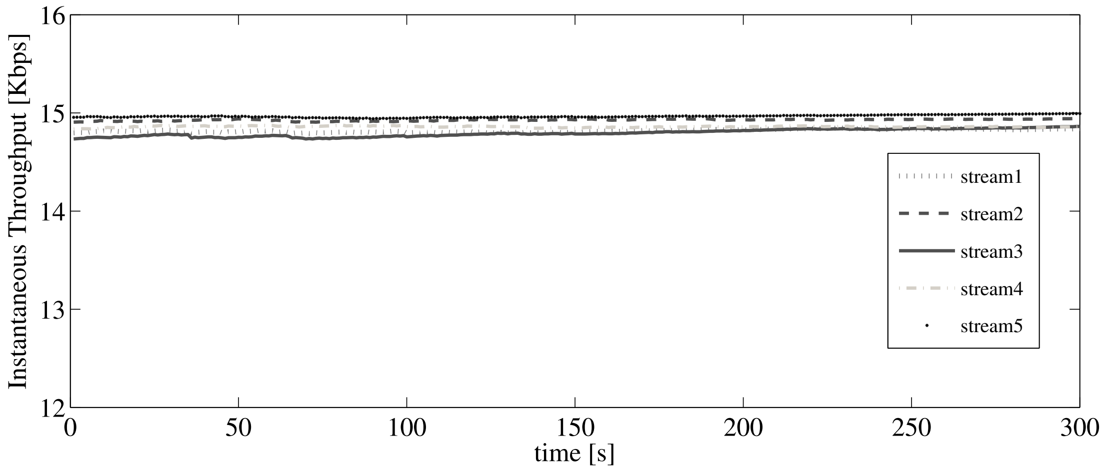


Figure 4.7: Instantaneous Throughput of 5 flow of same class.

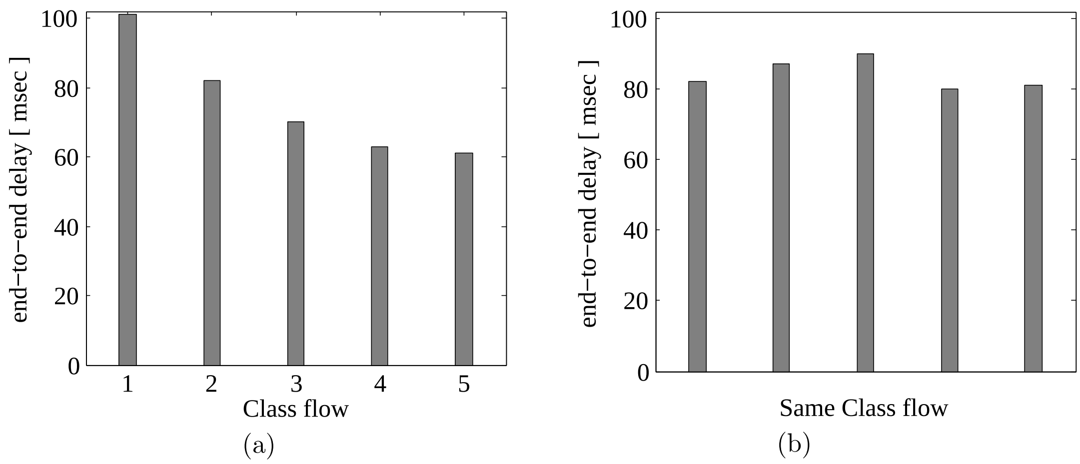


Figure 4.8: End-to-end delay for different class (a) and same-class (b) flows.

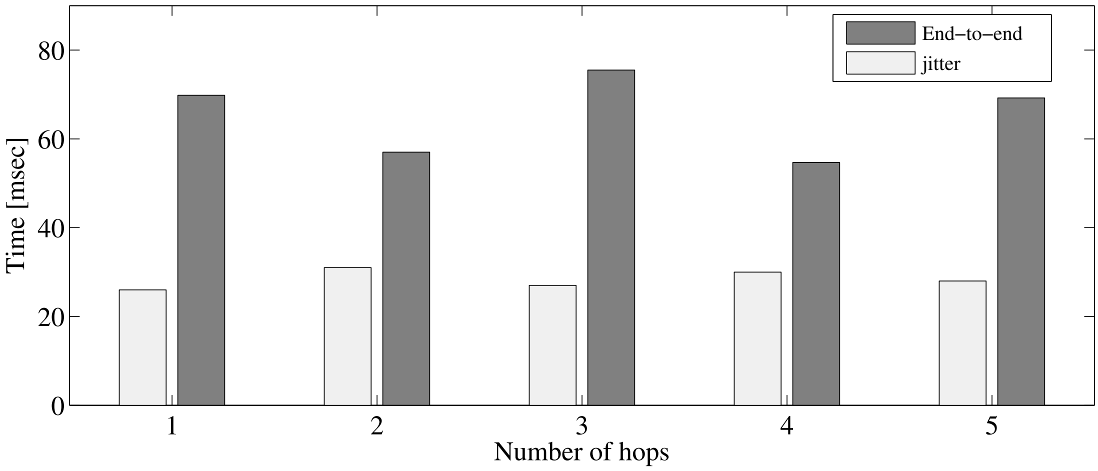


Figure 4.9: Delay and jitter vs hop count.

4.5.5 Multi-hop Transmission

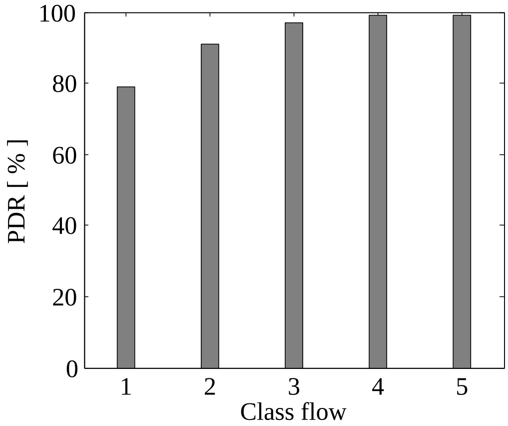
As was stated in section 4.3.3, the source and destination may be several hops away and most protocols do not take into consideration the number of hops a packet has to cross. Since QoS priority policy takes into account the hops remaining before a packet's destination, we have evaluated the end-to-end delay and the jitter of 5 flows when each node generates traffic with the same rate and same class flow to the furthest node. So the *hop left* of each one is different. The results are showed in Figure 4.9. Delays and jitters are small and the priority policy provides similar performances for the nearest and furthest nodes.

4.5.6 PDR Evaluation

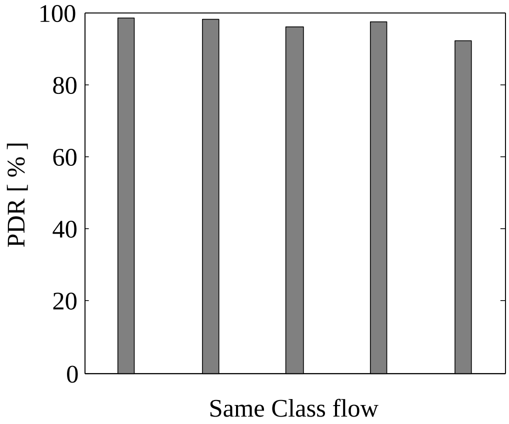
Packet Delivery Ratio (PDR) is a measure of the percentage of packets that reach the destination within the specified deadline. The PDR is calculated as the ratio of the number of packets received within the deadline by the destination application layer, and the number of packets sent by the application layer at the source node. Figure 4.10 shows PDR values for 5 flows of 15Kbps. In the first test (Figure 4.10.a), we generated flows with different classes. We repeated the test with the same class flows(Figure 4.10.b). The results show that the scheme gives acceptable PDR values and also show the effect of the priority policy.

4.6 Conclusions

In this chapter we have proposed a way to incorporate multimedia flows in a real-time wireless communication network without jeopardizing the real-time traffic. This idea has been implemented and analyzed as an extension of the RT-WMP



(a)



(b)

Figure 4.10: PDR for different class (a) and same-class (b) flows.

hard real-time protocol. This technique allows merging the real-time traffic with human communication such as video and voice over a MANET. The rationale is to take advantage of the bandwidth left free by the protocol when it is not working in the worst-case situation and use it to send QoS frames to allow audio and video streaming flows.

This QoS extension of the RT-WMP is perfectly integrated in the protocol and keeps real-time and QoS traffic separate and independent from each other. QoS messages are delivered following a priority policy based on flow class and laxity. The extension implements a flow admission control that estimates the available bandwidth using a distributed approach and allows or denies the entering of new flows into the system. The solution has been implemented over the RT-WMP and evaluated in a controlled environment, and the results show that it is a valid solution for adding QoS capabilities to real-time protocols. In fact, tests show that many audio and video flows can be supported simultaneously.

Further tests have been performed in real applications involving MESH networks and cooperative multi-robot teams, as presented in Chapter 6.

Chapter 5

Underground Propagation Issues

So far, we have presented the real-time and QoS characteristics of the RT-WMP protocol. As stated, protocol capability to route messages is based on reading the instantaneous quality of the link between nodes. This characteristic is essential in order to have a reliable view of the link status at the time of sending messages. However, this may not be enough especially in specific applications where the knowledge of the propagation evolution of the signal between the different nodes can be useful.

This is the case of confined environments such as tunnels or mines. These areas are interesting from the point of view of communications given that normal radio systems can provide at best very limited communications capability. As a result, the problem of providing an effective communications system in hostile environments, both for exploitation and emergency situations, has been an important issue in recent decades, particularly after a series of unfortunate underground disasters and accidents. Therefore, to utilize the MANET effectively, it is desirable to adapt the solution taking into account its effects on the signal propagation depending on the environment settings.

In order to provide radio coverage in long tunnels (railway, road or mines), the most commonly used systems are the so-called hybrid systems that combine wired and radiotransmission, like the Leaky Feeder (LF), and systems based on the natural propagation of radio-waves inside the tunnel. Due to the high cost of LF installations and the fact that they are susceptible to failures in disasters, the natural propagation system is preferred in many applications. If the carrier frequency is high enough such that the wavelength is much smaller than the cross-section dimensions of the tunnel, it behaves as a waveguide. In this case, the attenuation per unit length is low enough to allow communications over a range of several kilometers.

In this chapter we make a contribution towards the use of MANETs in underground settings. Following an empirical study, a set of real measurements carried out to validate theoretical results is presented together with an analysis of some signal propagation issues.

We consider the relation between the RSSI and the PDR, the transmission rate with respect to the area coverage, and the variation of the delay spread along the tunnel. We also show how the signal shape periodically exhibits slow and fast-fadings corresponding to such environment.

The collected data are evaluated in order to characterize the specific environment with a set of connectivity constraints with a view to implementing real underground communication applications that are presented in the next chapter.

Part of this work will be published in the special issues on Robotic Communications and Collaboration in Complex Environments of the International Journal of Robotics Research (IJRR) [Rizzo 13].

5.1 Related work

Although many different communication systems for underground areas exist, the most commonly used are those based on the use of radiating cables, such as the LF system, or wireless systems.

The Leaky Feeder cable is a hybrid system type. It is designed to allow the radio signal to "leak", both into and out of the cable [Delogne 82]. The properties and advantages of the LF have been evaluated in several works, as in [Nakamura 96] [Dekker 96]. However, it is still susceptible to single cable cuts, when a collapse can occurs.

Some studies began to question the robustness of traditional cable-based systems in terms of the tolerance of the communications components to harsh environmental conditions. For example, in [Einicke 97] the authors show how a solution based on Wireless Local Area Network (WLAN) can outperform a LF system in terms of the probability of maintaining communication when a disaster occurs.

However, electromagnetic waves do not propagate in tunnels as in free space, even if Line-of-Sight (LoS) is maintained between emitter and receiver. Many researchers have started to investigate wave propagation in confined environments to discover the reason for this strange behavior of electromagnetic waves. Thus, several studies about propagation, channel characterization and measurements have been carried out in the last decade.

In radio propagation modeling, two approaches are used: theoretical modeling and empirical modeling. Theoretical modeling is established by using either a modal approach or a geometrical optic approach. The modal approach poses some challenges in terms of its mathematical tractability. Tunnels are modeled as oversized imperfect waveguides. The received field is the sum of the fields consisting of a fundamental mode and a number of higher order modes, [Dudley 07, Sun 10]. This approach offers analytical expressions (i.e. solutions to Maxwell's equations), but only rectangular and circular cross section cases have been solved.

Moreover, since the shapes of galleries are not uniform and regular, the establishment of a general framework in theoretical modeling becomes even more complicated. In these cases, the geometrical optic approach can be adopted. This theory considers tunnel walls as reflecting planes. Propagation is achieved via a direct path and all possible reflected paths. The techniques proposed are Ray Launching [Hwang 98] and Ray Tracing [Seidel 94]. Neither technique can be used in the presence of curved surfaces, and a proposed solution is to tessellate geometries into multiple planar facets, as suggested in [Masson 09]. However, these methods could require overwhelming numerical calculations [Lienard 00].

Empirical modeling is based on extensive field measurements performed in the environment of interest. Collected data are evaluated in such a way that the statistical characterization of the radio propagation is obtained for that specific environment. Since empirical modeling characterizes the propagation statistically, the model obtained can be employed in similar environments. Due to the considerable effort, the difficulty of obtaining permissions and the safety issues involved, empirical approaches are not abundant in the literature. However, empirical approaches in underground mines have been attracting significant attention, and this has provided researchers with some opportunities to better characterize underground radio propagation channels.

5.2 MANET in underground settings

As we have said, the LF based networks are very costly to deploy and maintain and, in addition, they lack standardization. Moreover, in an emergency scenario (a collapse or similar) the system could be damaged and become useless.

Recently, wireless Ad-Hoc networks have been considered as an alternative solution [Yarkan 09] for providing communications in underground settings. They offer solutions to some of the fundamental challenges of all tethered communication systems such as easy maintenance (nodes can be installed, moved, removed and replaced easily), higher robustness against failures stemming from physical damage, mobility and low deployment costs. Therefore wireless systems using the 802.11 standard can offer a suitable way to interconnect nodes in underground mesh networks.

Although several studies about EM wave propagation have shown the substantial difference between confined spaces and free-space propagation, most of the valuable studies in the area of MANET have been performed by computer simulations or indoor experiments only. Thus, the lack of extensive testbed experiments together with the lack of accuracy of theoretical models means that the performance and behavior of MANETs working in hostile environments is not well understood. This is particularly true in tunnels, where real measurements can help to adapt a system to the environment in which it is to operate.

5.2.1 Link metrics consideration

Link quality measurement and estimation are a critical part of almost every mobile network routing protocol.

Several metrics are used for analyzing the quality of a wireless link, of which the most commonly used are the RSSI, SINR, PDR and the BER (see section 1.4).

There is currently an open debate on which to use and why [Vlavianos 08, Wu 08] due to the fact that each metric represents a different characteristic. The conclusion is that there is no single metric to measure everything required, in order to establish the quality of a wireless link.

Given that commercial hardware does not provide noise information while receiving packets but only an average estimation, it is quite hard to compute the SINR metric. On the other hand, the use of PDR involves substantial latency for link quality estimation [Souryal 06]. BER computation introduces significant overheads and is sensitive to bit sequences [Vlavianos 08]. Finally, RSSI does not capture the amount of destructive interference in links and it could lack accuracy at high transmission rates due to its being measured at the lowest rate (during the reception of a packetpreamble).

Analyzing the validity of common assumptions with regard to each metric, it is apparent that each of them provides an estimation of the link quality over a period of time with limitations in terms of accuracy. No single metric on its own can be considered sufficient to accurately characterize the quality of a link.

However, RSSI can be a promising metric when its value is above the sensitivity threshold [Srinivasan 06] and the application requirements in terms of transmission rate are not high [Holland 01]. Furthermore, the use of a token-passing protocol (as in our case, the RTWMP protocol) which prevents simultaneous transmissions, relieve the negative effect of interference in the measurement of this metric.

PDR could depend on the packet size and the transmission rate. That said, however, the PDR can characterize the link quality if only a few types of packets are used and assuming that the transmission rate is fixed.

Moreover, RSSI and PDR metrics are not independent of each other. For example while PDR does not measure power, it is correlated with RSSI at certain transmission speeds [Vlavianos 08]. These relations have been studied in order to identify appropriate combinations for determining the quality of a wireless link in an effective manner.

5.3 Environment - The Somport tunnel

The Somport tunnel was selected as the location for carrying out the analysis and the majority of the experiments presented in this work. This is an old railway tunnel representative of long straight tunnels common in transport or mine ap-

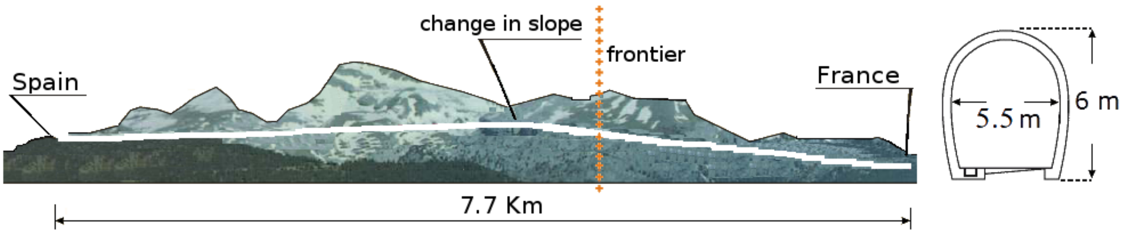


Figure 5.1: The Somport tunnel.

plications. The 7.7 Km railway tunnel connects Spain with France through the central Pyrenees. It has a horseshoe-shape cross section, 6 meters high and 5.5 meters wide. The tunnel is straight but there is a change in slope at approximately 4 kilometers from the Spanish entrance, as can be observed in Figure 5.1. The walls are made of limestone, with relative permittivity $\epsilon_r = 5$ and relative conductivity $\sigma = 0.01\ S/m$.

The tunnel has some particular features, such as small vaults every 25 meters. These are 1 meter wide, 1.5 meters high, and 0.6 meters in depth. It also has 17 lateral galleries, of more than 100 meters each, of the same height as the tunnel.

In the next section, we explain the metrics and the rate selected in order to measure and then analyze the communication signal propagated in the tunnel.

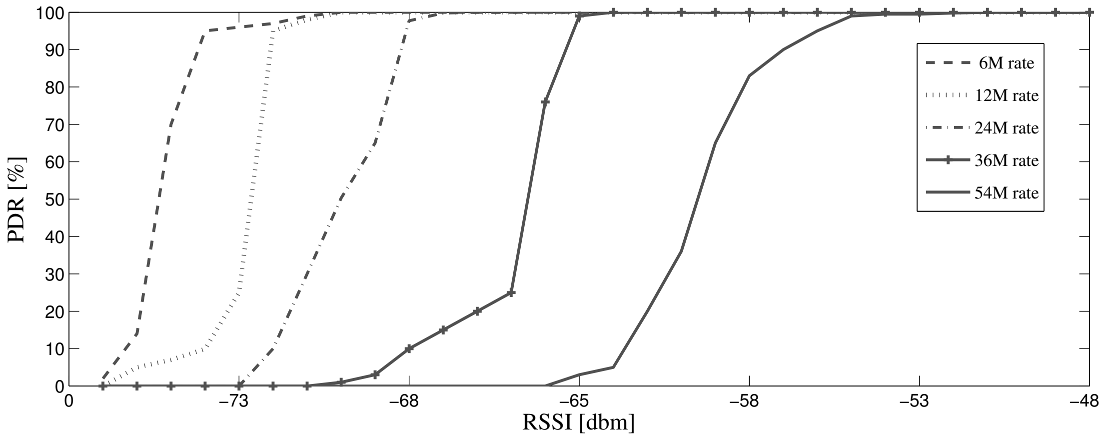
5.3.1 RSSI and PDR relation

PDR tends to decrease for higher transmission rates, since higher rates are more vulnerable to external noise and interference. In order to validate that using the RT-WMP protocol, we consider an experiment in which, a node in our testbed takes turns in unicast traffic (in isolation) and another node records the RSSI values from the received packets. We conducted experiments with all possible fixed rates.

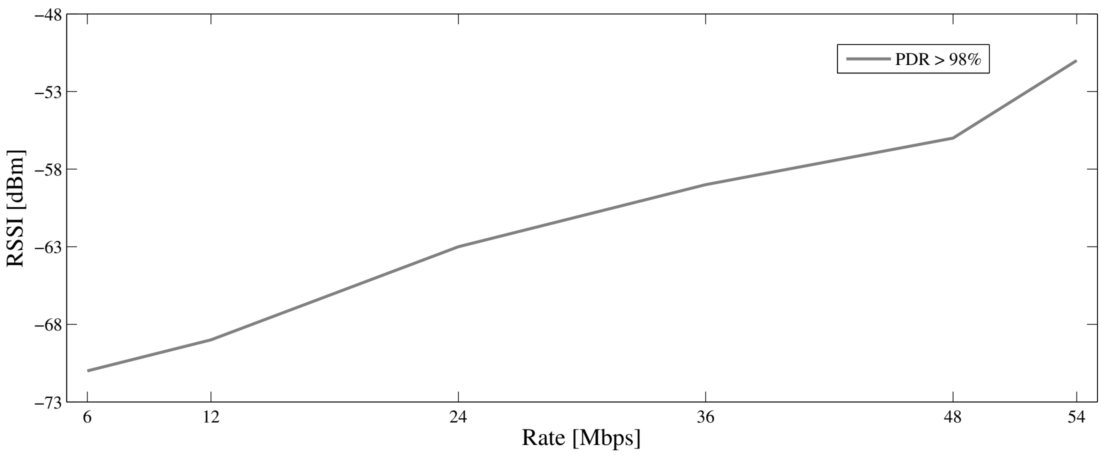
Figure 5.2 presents a plot of the PDR versus the RSSI for five different rates from which we can observe the correlation between the two metrics. In particular, Figure 5.2.b highlights how at high bit rate transmission, a suitable PDR level is lead only of the node links that show stronger RSSI levels. This relation assumes importance when there is a need to ensure a certain level of QoS. For example, working at a rate of 54M, achieves a level of quality in terms of PDR which would not be attainable for modest values of signal intensity. In other terms, this correlation allows us to estimate a qualitative metric, the PDR, through the quantitative parameter RSSI.

5.3.2 Rate and Coverage Range

Another aspect to take into account is the well known relation between the range and rate of WLANs. Notice that lower rate transmission schemes have greater transmission ranges than higher rate schemes [Rappaport 96, Holland 01]. This



(a)



(b)

Figure 5.2: Empirical relation between RSSI and PDR measured. In (a), the variation for five different transmission rates. In (b), figure highlights the RSSI and Rate values that correspond to acceptable PDR level.

is even more true in confined environments such as tunnels where, at the typical WLAN carrier frequency, the tunnel acts as a waveguide.

In order to validate that relation, we conducted an experiment similar to the previous one but this time considering a node moving along the tunnel while recording the RSSI values from the received packets. We wanted to compare the coverage range for a 6 Mbps and a 54 Mbps data rate. Figure 5.3 shows the results which confirm the cited rate-coverage relation. By setting the same transmission power, in the 6 Mbps rate configuration, good RSSI values are obtained along more than 2 km away and practically no packets loss occur. Instead, the 54 Mbps rate schema already suffers a heavy packet loss from the first 200 meters.

The conclusion is that in certain specific applications (such as rescue or exploration), maximizing bandwidth is not able to meet more strict requirements such

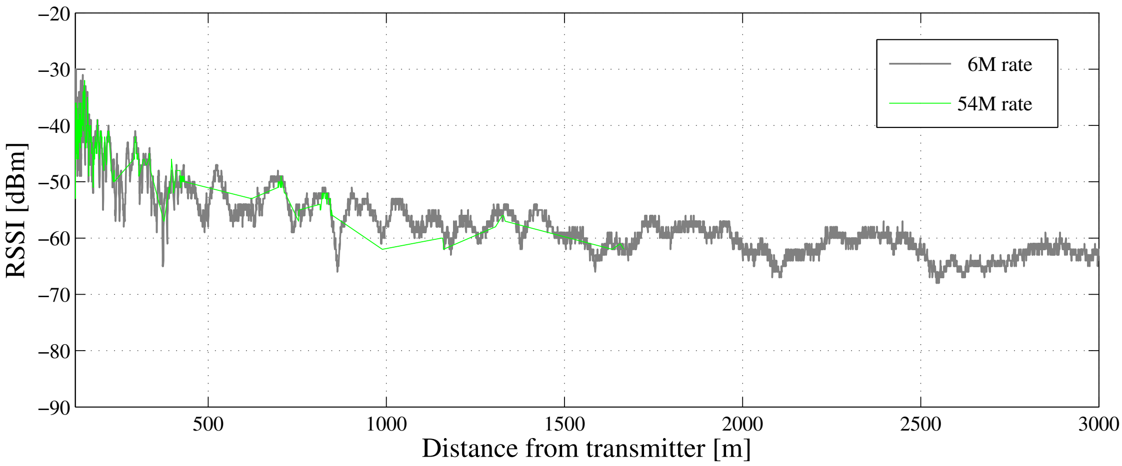


Figure 5.3: Coverage range for 6 Mbps and 54 Mbps data rate along tunnel.

as link quality and coverage range. Considering this, we fixed the operating rate in the testbeds presented in this work at 6 Mbps.

5.3.3 Fading Analisys

Propagation in tunnels is affected by the multipath effect. The latter is the main factor responsible for strong *fading* phenomena that affect both the intensity and the quality of the signal that reaches a receiver. These phenomena have been studied by many authors. In [Lienard 98], the fading phenomena of tunnels are statistically analyzed. They are classified in short-term (also referred to as *fast-fadings*) and long-term (*slow-fadings*), and three regions are established where fadings behave differently: 0 - 50 meters, 50 - 500 meters and beyond 500 meters from the emitter. The prediction of radio coverage levels is required to develop communication systems and optimize their deployment ensuring availability and robustness of the radio links. Several theoretical modeling approaches have been proposed, as stated in Section 5.1, and some experimental studies have been made to establish their accuracy. See, for example, [Masson 09] for ray optics theory or [Sun 10] for modal theory. It is clear that none of the techniques can predict with sufficient precision the position or magnitude of a fading.

Thus, taking into account the fading phenomena effect, experiments performed in underground environments cannot be based only on a theoretical model. In order to study longitudinal variations of the signal, we performed a set of real measurements. The transmitter was placed 0.25 meters apart from the wall and 2 meters above the ground. One moving-receiver' antenna was placed at a height of 1.80 meters and a distance of 0.60 meters from the tunnel axis. It was displaced from the transmitter position up to 2900 meters, maintaining the line-of-sight between them. The signal was sampled with a spatial period of 0.1 meters. The result is shown in Figure 5.4.

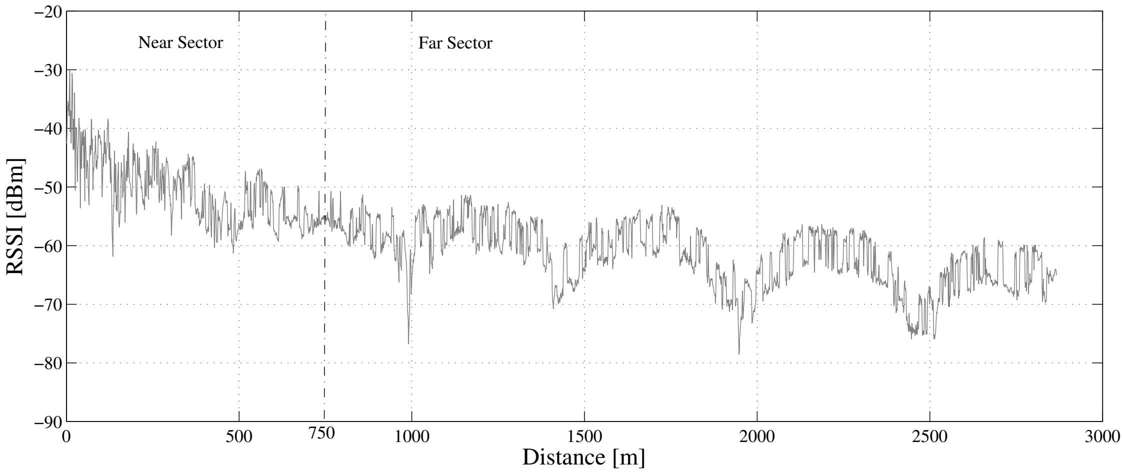


Figure 5.4: Measured received power (dBm) along tunnel.

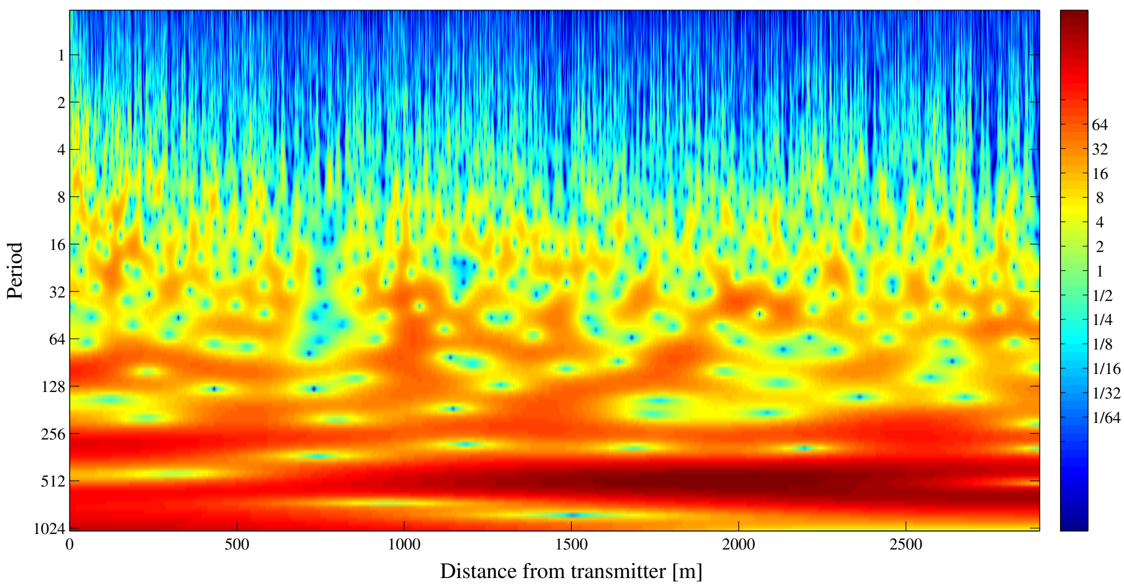


Figure 5.5: Wavelet of the signal versus the distance using the Morlet function.

As can be observed, two main sectors can be identified in the tunnel according to the signal behavior. The boundary between the sectors is at a point around 750 meters from the emitter. In the first sector (*near sector*) very fast fluctuations of the signal power (the fast-fadings) and the distance path loss dominate. In the second sector (*far sector*), the slow-fadings dominate instead.

To analyze this different behavior, the wavelet of the signal as a function of the distance is presented in Figure 5.5. To calculate the wavelet, the signal series was padded by mirroring the ends in order to minimize the border effects.

The wavelet shows that the behavior changes at 750 meters. In the near sector

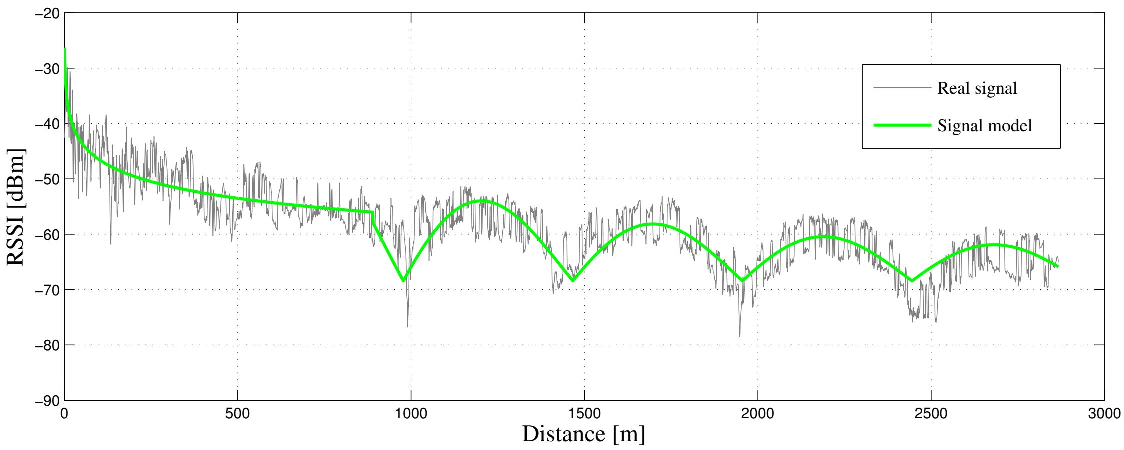


Figure 5.6: Real signal and signal from the model.

the spectral power is distributed along all spatial frequencies, including high frequency components. Nonetheless, in the far sector, the low frequency components are concentrated in a band around 512 meters of period. This band highlights the existence of slow-fadings. Besides, in this sector the fast-fadings exhibit a similar frequential behavior as in the near sector.

As we can see, in the near sector, apart from the fast-fadings, the distance path loss dominates following a logarithmic decay in terms of power. In the far sector, the signal power exhibits a characteristic shape (see Figure 5.4) which evokes a typical $Sinc$ function.

Considering the real data, we tuned such a mathematical function to reflect a similar behavior for $y(x)$ where

$$y(x) = k \cdot \left| \frac{sin(\frac{\pi}{\lambda} \cdot x)}{x} \right| + c \tag{5.1}$$

λ being the spatial period of the signal and k and c tuning parameters. A least squares optimization technique has been used to find the optimal parameters k, λ and c to fit the real data with the artificial curve. In Figure 5.6 the measured and the computed signals are shown.

In this way we obtain an artificially designed signal that can be used as a model for simulating the real signal propagation. This could be useful when simulation or real testbed experiments (not in an actual fading environment) have to be performed.

5.3.4 Delay Spread Measurement

The delay spread is used mainly in the characterization of wireless multipath channels. It can be interpreted as the difference between the time of arrival of the

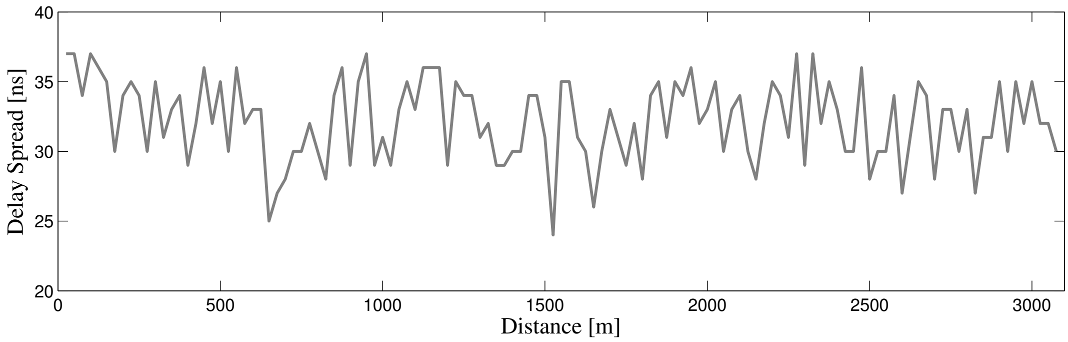


Figure 5.7: Delay Spread values sensed from receiver.

earliest significant multipath component and the time of arrival of the latest multipath component. In [Nerguizian 05], extensive channel characterization is made by measurements of the delay spread and the coherence bandwidth in a mine. The results show that the channel does not follow a dual-slope relation with respect to the distance. Similar channel measurements are presented in [Benzakour 04], analyzing both 2.4 and 5.8 GHz. The results show that indoor multipath characteristics can strongly depend on the node separation and the dimensions of the gallery.

In order to validate the results cited above, we performed a test to measure delay spread along the tunnel. The test is useful for obtaining information about the best places to locate the backbone nodes, avoiding zones affected by fading or interference.

We measured the RMS delay spread using the YellowJacket Tablet Wi-Fi analyzer (Berkeley Varitronics Systems). The measurements were repeated every 25 meters over 3.2 km of the tunnel and the results are shown in Figure 5.7. As expected, the delay spread oscillates between 25 ns and 38 ns approximately, showing similar values to those calculated in experiments carried out in similar environments (see [Aikio 98] and [Lienard 99], for example) and slightly higher values than than the usual values of around 20 ns found in empty tunnels [Molisch 11].

5.4 Conclusions

Although there are several communication systems for underground mines, wireless communication attracts considerably more attention than the others. Recently, MANETs have been considered as an alternative solution for providing communication in these areas. However, the mere application of a protocol that does not take into account the signal propagation in this specific environment may not be enough in order to provide a reliable network.

The contribution of this chapter lies in an empirical signal analysis carried out in a real environment, the old Somport railway tunnel connecting Spain and France through the central Pyrenees. The propagation analysis results have led to the formulation of a useful set of considerations in view of experiments.

Firstly, we have considered the relation between the RSSI and the PDR. This allows to identify a threshold of the degree of reliability of a link between two or more nodes.

Secondly, it is shown how a low transmission rate is preferable to obtain a greater degree of area coverage. In addition, we have evaluated the variation of the power sensed and the delay spread along the tunnel. Such information can be used, for example, to provide an efficient deployment of a set of fixed nodes offering multi-hop coverage.

Finally, we have verified that the tunnel exhibits the general characteristics corresponding to a fading environment, with periodically slow and fast-fadings. This signal shape suggests that taking these characteristics into account is effective for developing a strategy to deploy mobile nodes along a tunnel, such as autonomous robots for exploration purposes.

Applications of this analysis are described in Chapter 6.

Chapter 6

Applications

Just ten years ago, the idea of ad-hoc nodes providing connectivity and capability where needed or a team of robots forming a multimedia network incorporating remote visualization and control were still imaginary scenarios [Ramanathan 02].

Nowadays, improvements in technology and research mean that these scenarios are ripe for the development of increasingly complex systems. However, much research proposes isolated solutions and relies on simulation only. There is a lack of convergence of various disciplines towards the integration of systems for real applications.

This chapter describes a set of applications in real scenarios that cover various aspects of ad-hoc networks, robotics applications and the effects of the environment.

An assessment of the communication protocol between a pair of mobile nodes in a confined environment is presented. An experimental application involving real robots and human operators undertaking a real exploration in a tunnel is described. This application involves a planning technique based on the use of the characteristic parameters in fading environments for the deployment of a team of robots.

6.1 Real-Time protocol in underground voice communication

How we stated in Chapter 5, due to the nature of the environments and to the electromagnetic waves propagation, communication in tunnels and mines is very challenging. The used systems are often unidirectionals (e.g. in mines) or very costly (e.g. LF in road tunnels) and hard to install and maintain.

In this section, the use of multi-hop ad-hoc networks to provide multimedia communication between mobile nodes in such hostile environments is proposed, relying on a complete hardware/software easy-to-setup platform that can be used both as temporary or fixed infrastructure or as communication backbone in emergency scenarios like mine accidents or a tunnel collapse.

In order to achieve this purpose, the communication is based on the RT-WMP protocol and its QoS extension, described in Chapters 2 and 4 respectively and the implementation is carried out by a type Wireless Mesh Network (WMN) over several nodes equipped with a specific embedded-PC hardware.

The main contributions of this work deal with to the signal propagation, nodes deployment, efficient routing, node mobility and implementation. A previous analisys of the propagation in tunnel, exposed in Chapter 5, allows to positioning the backbone nodes in order to minimize de multipath effect. The specific topology and situation have driven to a specialization of the RT-WMP protocol to better perform routing messages in this type of environments(taking advantage of the a priori knowledge about the topology) and supporting the mobility of the ends nodes. The result system is a novel flexible infrastructure constituted by a set of backbone nodes placed in the confined environment at strategic points and a set of mobile nodes that can move maintaining the voice link among them.

Part of this work was sent at the third International Conference on Wireless Communications in Underground and Confined Areas [Sicignano 10c], while the complete results were published in the Ad Hoc Networks international journal [Sicignano 11].

6.1.1 Related works

In confined and underground areas such as tunnel or mines, WMNs have emerged as a technology solution [Akyildiz 05]. This kind of network provides a wireless backbone formed by fixed relay nodes for mobile users to access the infrastructure or communicate with each other. Due to the shape of these confined environment, chain topologies are very useful. Nodes are fixed and each node can only communicate with its predecessor and its successor in the chain.

In [Einicke 97], authors show the benefits of using solution based on WLAN backbones can outperform a cable solutions as LF in terms of probability having communications available, when any disaster can occur. In [Aisa 10], authors propose the WICKPro protocol, a Real-Time protocol using a token-passing ap-

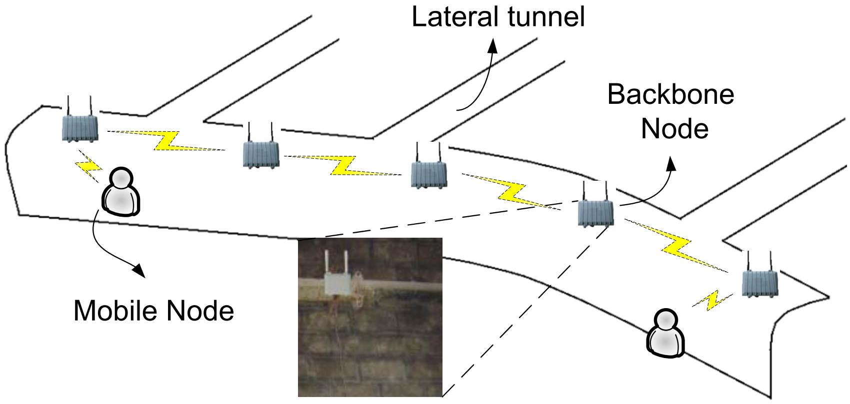


Figure 6.1: The environment.

proach and PDR metric, specifically designed for WMNs with chain topologies which. Other works, based on 802.11 networks, analyze different aspects of the underground multimedia communication. An approach for video transmission in a mine providing statistics about packet losses suffered is proposed in [Beaudoin 04]. In [Moutairou 06] a work that proposes a technique to optimize the mesh access points location is presented. [Aniss 04] proposes a hybrid solution that tries to adapt the 802.11 standard to underground communications. The network is a combination of the wireless standard with the DOCSIS data-over-cable standard used as a backbone.

However, as explained in Chapter 5, although the 802.11 networks have been extensively tested in outdor and indoor areas, very few performance measurements have been performed in tunnels or mines and its limitations in terms signal propagation in these environments are not take into account. Moreover, WMN limitations in terms of multi-hop routing and Quality of Service (QoS) support are also not considered. This last issue has been deeply studied thanks to the growing interest on offering multimedia contents in MANET networks, as exposed in Chapter 4.

In short, none of literature proposal offers a complete, flexible and cheap platform to offer communication in underground areas.

6.1.2 Specialization on the environment

The RT-WMP has been designed principally to support real-time communication in teams of robots and thus to give support to any type of topology that can appear due to node mobility, and its routing algorithm was developed to work in this situation. However, the environment considered here is quite different. We have basically a n backbone nodes and m (= 2, at the moment) mobile nodes, and we can take advantage of this previous knowledge to design a more efficient routing algorithm and improve the mobility characteristics of RT-WMP. The multi-hop chain topology is shown in Figure 6.1.

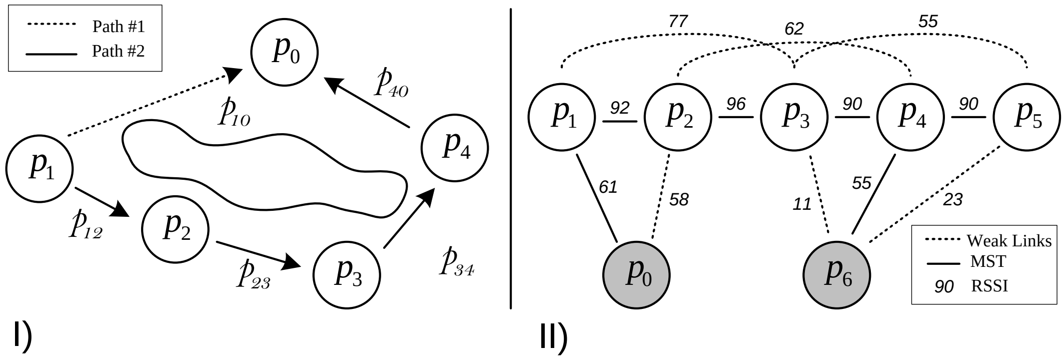


Figure 6.2: Alternative paths to reach the same node.

Using the Minimum Spanning Tree

In the RT-WMP, frames are routed using the LQM taking into account either the link quality of the nodes and the distance to the destination node. To each link is assigned a cost depending on the corresponding value of the LQM. The Node choses the less costly path to reach the destination. Depending on the link-quality topology of the network, the chosen path can be the shortest but even the longer. The heuristics behind the routing algorithm, in fact, tries to reach a comprimise between the options of sending frames over weak links and using a longer path. Let consider Figure 6.2.I. We have two options to deliver a message: if we chose the first path, the destination node is only a hop away while in chosing the second destination is 4 hops away. The probability of error is:

$$p_{p1} = (1 - p_{10}), \tag{6.1}$$

using path #1, while:

$$p_{p2} = (1 - p_{12}) \cdot (1 - p_{23}) \cdot (1 - p_{34}) \cdot (1 - p_{40}) \tag{6.2}$$

using path #2, p_{xy} being the propability of transmission error in the link between node p_x and p_y that, in turn, is calculated as a function of the RSSI.

There could be therefore situations in which a shortest path is considered safer than a longer one even if in the latter, links are all stronger. This behavior is desirable in generic networks (e.g. a team of robots uniformly distributed). However, in situations in which (part of) the topology is known, the routing algorithm can be improved to obtain a safer behavior. In tunnels, for example, the backbones nodes are placed in strategic points to guarantee a good and, above all, symmetric link among them. Moreover, they use to have a high-gain antenna and the transmission power is substantially greater than the power of the mobile nodes. It implies that the probability of communication error between adjacent nodes is very low, almost negligible.

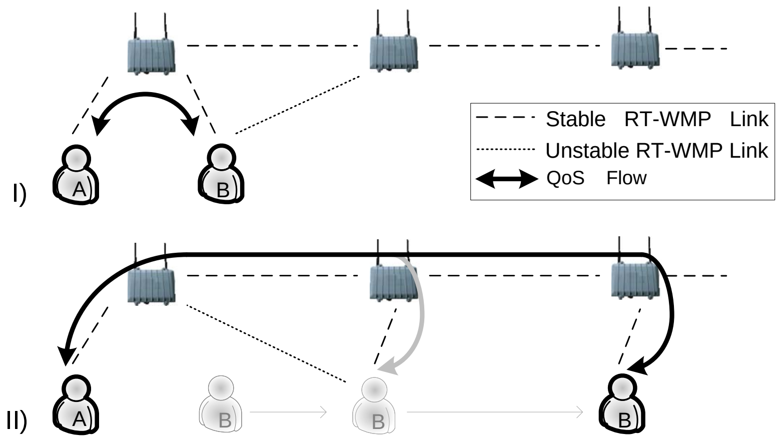


Figure 6.3: An illustration of mobility scheme.

We decided, thus, to force the protocol to use backbone nodes for backbone communication and mobile nodes to link itself to the closest (in terms of link quality) backbone node. In order to achieve that, we reduced the topology of the network to a spanning tree where only the best links are selected or, more concretely, to a minimum spanning tree applying the Prim's algorithm to the LQM [Tardioli 12b]. Figure 6.2.II shows the results of this process. The backbone topology of the network becomes a string and the node to communicate using the best possible link with the backbone. The rationale is that the nodes see the network as a tree whose branches are the best possible links. An example of how this new scheme works is given in Figure 6.3. As we can see in Figure 6.3.I, the link quality between nodes A and B enables a stable connection between the mobiles nodes (A and B) and the backbone node while the weak link are ruled out by the Prim's algorithm. While B is moving across the tunnel (Figure 6.3.II), the protocol manages the link quality change allowing multi-hop re-routing across the network and guaranteeing a connection all the time.

Since routing, as explained, is based on current and real signal quality, in some situations (even if this is not common) a mobile node can act as a bridge between two backbone nodes.

6.1.3 Evaluation

The main experiment was performed in the Somport (see Section 5.3). The tunnel was closed to traffic, so we can assume the experiments were made in stationary conditions. Tests have been done along about 7.5 kilometers.

Five nodes equipped with minimal embedded and dedicated hardware (100x160 mm PcEngines ALIX3D3 board, battery powered) and Atheros chipset-based wireless cards and running the MaRTE OS [?] implementation of RT-WMP, were distributed along the tunnel and used as backbone nodes. In addition, two laptop computers running Linux OS were used as mobile nodes.

The voice was sampled at 8 Khz and 16 bit per sample and was compressed using the *speex* [RFC5574 09] codec to obtain a full-duplex communication of 15 Kbps bandwidth for each flow. Each RT-WMP-QoS message contained four speex voice packets. The packets' deadline was fixed to $150ms$ following the ITU-T recomendations [ITU-T 03].

Before performing the final test, however, we made a set of additional experiments to investigate the environment in which the experiment had to take place and chose the adequate parameters to obtain satisfactory results.

The first test was about the measurement of RSSI and Delay Spread along the tunnel to obtain information about the best places where to put the backbone nodes avoiding zones affected by fading or interferences. The second set of tests have been performed to discover the best parameters to obtain a correct and effective voice communication in terms of packet aggregation (the number of voice data packet to be transmitted at a time) and reception queue size. Finally we verified the new routing algorithm in an indoor test.

The next sections describe these preliminary test and its results.

RSSI and Delay Spread Measurement

As we stated in Chapter 5, tunnel acts as a waveguide with a cut-off frequency below which no effective propagation occurs. In this case we are above such a cut-off frequency and is thus possible to take advantage of this effect to obtain greater communication ranges than in open space.

Using the measures defined in the Section 5.3.3 and Section 5.3.4 to evaluate the variation of the power sensed and the Delay Spread by a receiver, we consider the effect of the multipath and the fading. The mean radio-signal decreases with distance but the fading has a strong presence both in terms of RSSI and Delay Spread that oscillates between 25 ns and 38 ns aproximatively

The RSSI is influenced also by the presence of lateral galleries that affect the received signal, producing a sharp fall in the signal intensity in correspondence of the mouths. On the other hand, the waveguide effect allows higher RSSI values along the tunnel than in open space.

These aspects have been taken in account in the deployment operations since we wished to provide an efficient multi-hop coverage of the communication. The idea is to deploy backbone nodes in order to optimize the transmission in the tunnel taking advantage of one of the peaks that are visible in the Figure 5.4 and avoiding, instead, the Delay Spread peaks visible in the Figure 5.7.

Parameters chosing

To obtain a continuous flow without cuts or interruption, voice packet must be exchanged among mobile nodes with and adequate frequency and within its deadline. It means that if we are able to deliver a message each 50 ms, for instance,

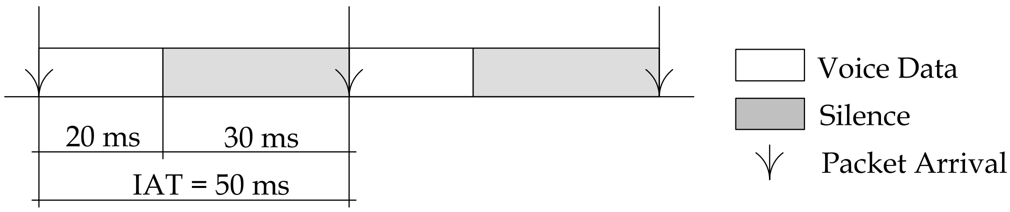


Figure 6.4: Relation between voice data and inter-arrival time.

the packet must contain *at least* 50 ms of voice. On the contrary, if the packet contains insufficient data (e.g. 20 ms of voice) the listener will hear silence until the arrival of the subsequent packet (see Figure 6.4). We have, thus, to consider the Inter-Arrival Time (IAT) that the communication network is able to provide to decide how much voice data have to be transported within a single packet. We made a first indoor experiment to determine this. We arranged a seven nodes *chain* network (providing the nodes with a fake LQM) and saturated the network with two end-to-end QoS flows. Figure 6.5 presents both the distribution and the temporary shape of the IAT of the voice packet. The image shows three major peaks, the last of which around the 70 ms and a very small one at about 150 ms. It means that in general we must be able to send at least 70 ms of voice every 70 ms. Moreover the peaks tell us that in some rare circumstances we'll receive packets 150 ms apart. Since the speex codec, in the configuration used in these experiments, generates data packets containing 20 ms of voice, we whould send:

$$n_{packets} = \left\lceil \frac{70}{20} \right\rceil = 4 \tag{6.3}$$

packets in each loop. On the other hand to absorbe sporadic high IATs, we should have a queue of:

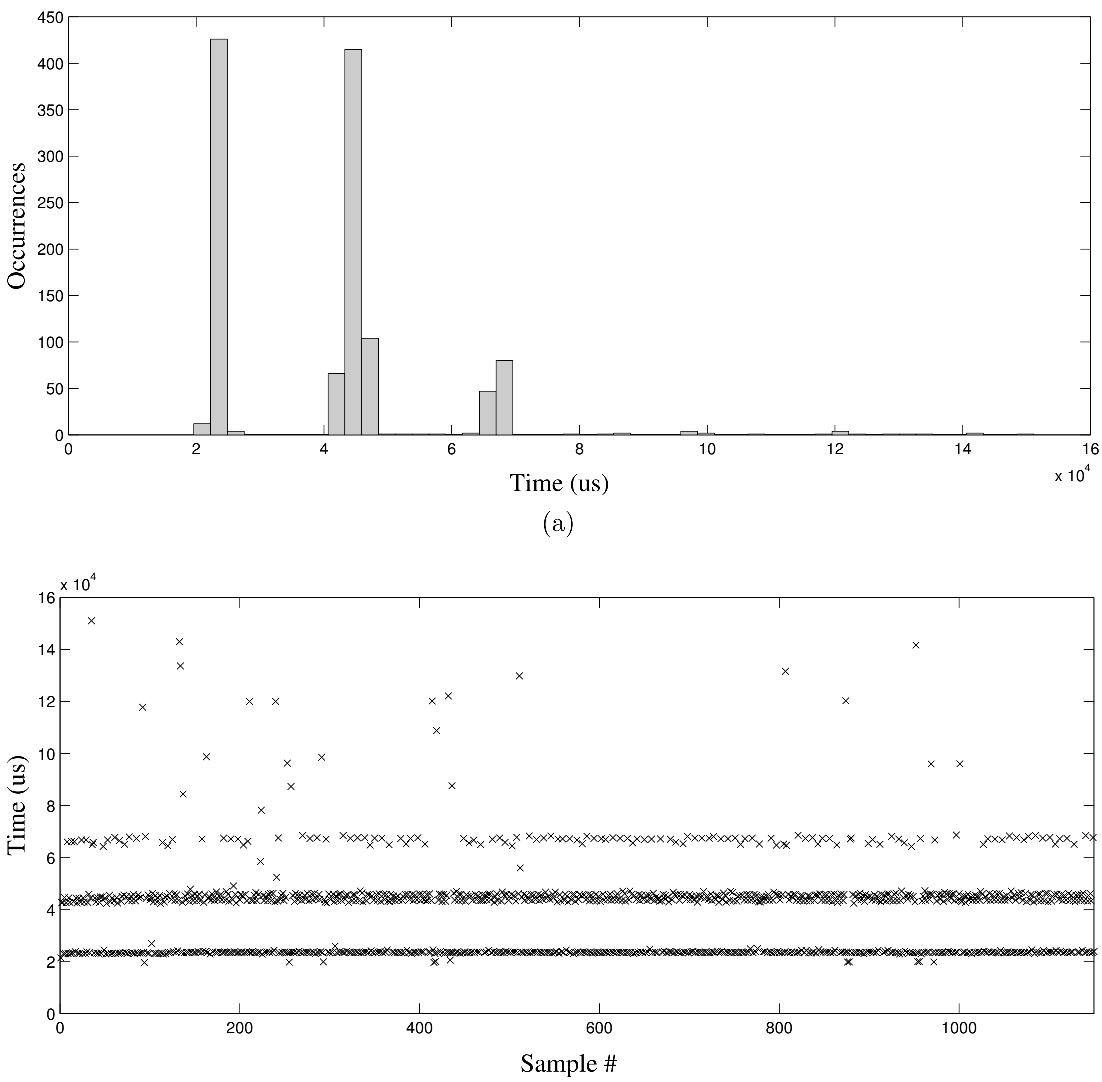
$$n_{queue} = \left\lceil \frac{150}{20} \right\rceil = 8 \tag{6.4}$$

packets. This queue will introduce a delay of:

$$delay_{queue} = n_{queue} \cdot 20ms = 8 \cdot 20ms = 160ms \tag{6.5}$$

that must be added to the mouth-to-hear end-to-end delay of the packets. This value is however assumable as guaranteed by the ITU-T recomendations [ITU-T 03].

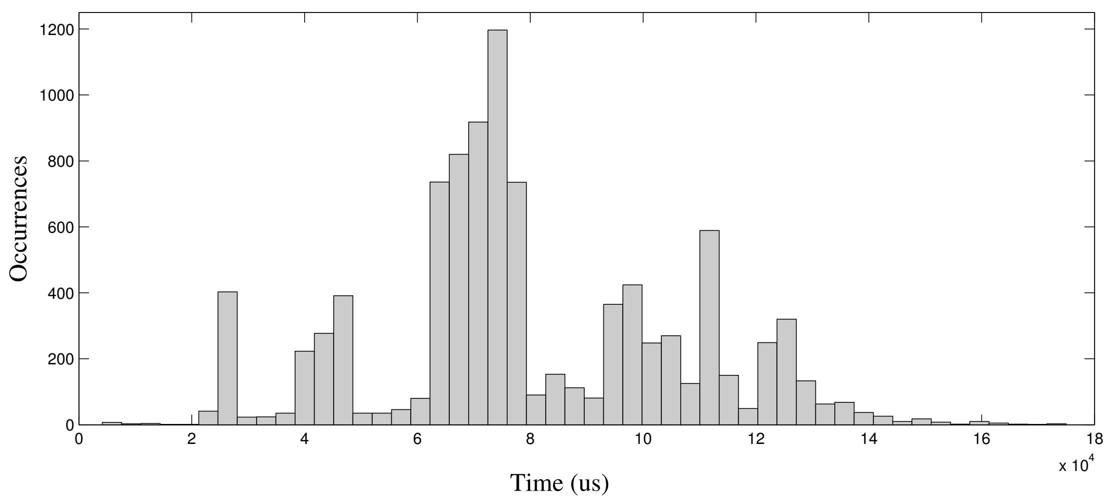
We tested the goodness of these parameters with another indoor experiment, using two real voice flows (128 Kbps each one before compression, about 15 Kbps after *speex* compression). This time, a movement of one of the nodes (node 0) was simulated through the dynamic modification of the fake LQM. The RSSI provided to the nodes was calculated as a function of the simulated distance and perturbated with a 20% of noise to obtain a similar situation to the real. Moreover all the nodes



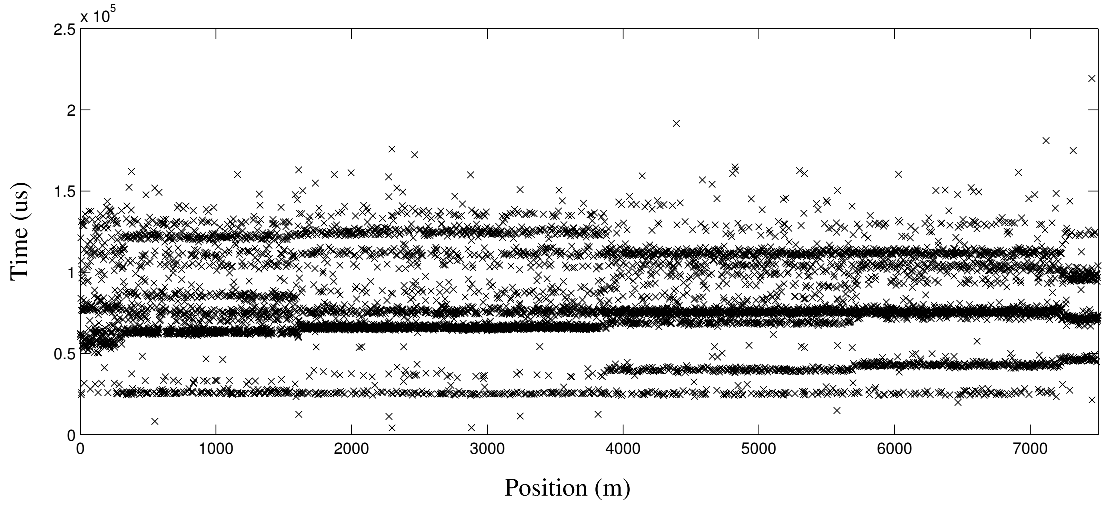
(a)

(b)

Figure 6.5: Distribution (a) and raw data of Inter-Arrival Time (IAT) (b) for two saturated flows.



(a)



(b)

Figure 6.6: Distribution (a) and raw data of Inter-Arrival Time (IAT) (b) .

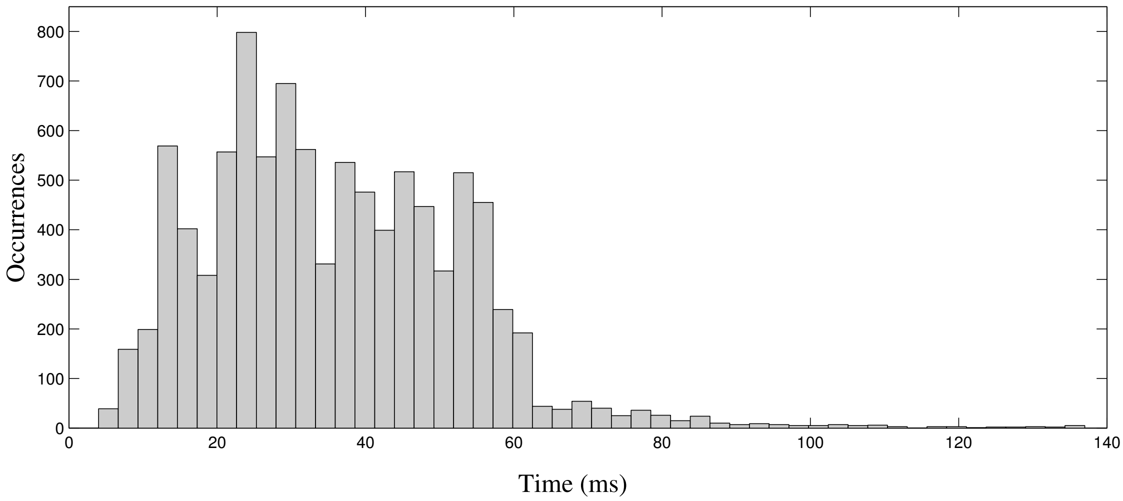


Figure 6.7: End-to-end delay distribution.

ignored all the frames that, in a real situation, would not have received due to the excessive distance.

Figure 6.6 presents the results of the test. The histogram shows now several peaks which one most important is at about 70 ms. The plot shows that the distribution approximately constant along the whole experiment even if this graph give us the information that the peak at 130 ms in the previous figure corresponds principally to the first half of the experiment while the one at 42 ms to the second half. It is due to the reconfiguration of the network during the movement that promotes different delivery paths.

On the other hand, the analisys of the end-to-end delay (see Figure 6.7) suggests that the packets honour its deadline since the most part of the packets are delivered in an interval between few milliseconds and 100 ms guaranteeing the correct playback of the voice at the destination node. As expected, no packets were delivered beyond its deadline (150 ms).

RSSI and Prim Based Routing

The same experiment gave us information about the effectiveness of the RSSI and Prim based routing. Figure 6.8 shows its behavior. The figure is referred to mobile node 0 and shows the identity of the last-hop sender (that is, the identity of the node that delivered the message to node 0) and the RSSI, considered as indicator of the link quality in this article, with which the first listens the latter (see figure 6.9).

The two mobile nodes (0 and 6) start closely each other and to the node 5. Several frames are exchanged directly among the node 0 and node 6. Then, node 0 starts moving toward the other end of the backbone. The link quality with

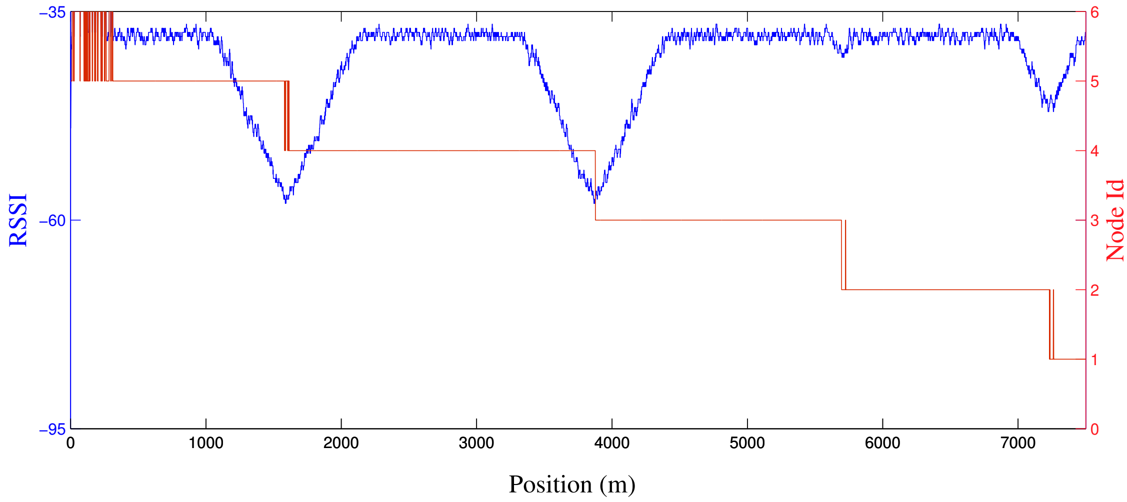


Figure 6.8: RSSI and Prim based routing simulation.

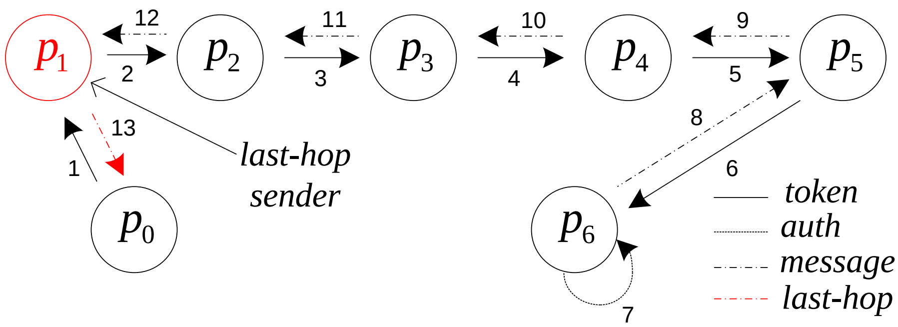


Figure 6.9: Identity of the last-hop sender.

node 6 falls and node 0 begins to exchange frames with node 5 following the rules marked by the Prim's algorithm. The same occurs with the subsequent nodes. As expected, the link quality with the sender is always maintained at acceptable values. The algorithm suffers from short oscillations in the switching point due to RSSI noise that are, however, completely assumible by the system. In some situation, moreover, node 0 acts as a bridge between adjacent nodes again due to the RSSI fluctuation.

6.1.4 Real experiment

The real experiment consisted in the deployment of the cited five nodes. Table 6.1.a lists the parameter values used in the tests while table 6.1.b shows where the backbone nodes have been deployed along the tunnel in order to provide a suitable inter-backbone node RSSI value.

The third node position, however, was chosen in the peak nearest to the tunnel

	Parameter	Values
Scenario	Frequency	2.412 GHz
	Channel rate	6 Mbps
	Tx Power	100 mW
Data	Pkt size	160 Byte
	QoS flow rate	15 Kbps
Constraints	Deadline	150 ms

(a)

	Position [m]
Nodes 1 - 2	≈ 2000
Nodes 2 - 3	≈ 2000
Nodes 3 - 4	≈ 1200
Nodes 4 - 5	≈ 1500

(b)

Table 6.1: Parameters used in the real tests.

	Flow 1	Flow 2
PDR [%]	98.2 %	97.9%
MOS	> 3.5	> 3.5

Table 6.2: Main testbed results.

slope change. In this way we guaranteed the presence of LoS between each couple of nodes. Especially, the third node act as relay between the left-side and the right-side of the chain that have not LoS between them due to the change in slope.

Two laptops running Linux OS were used as mobile nodes. The sampling of the voice signal was performed accesing directly the */dev/dsp* device and compressing 320 byte of data (160 samples of 16 bit) to a 40 bytes speex packet (20 ms of voice). Packets were aggregated in groups of four and sent to the other mobile node and as in the laboratory experiment, the QoS extension was configured to transport up to two QoS messages in each protocol loop (see [Sicignano 10b] for details). One of the mobile nodes was maintained still at about 400 m apart from one of the backbone end while the other was moved, within a car, toward the other end of the backbone maintaining in any moment the voice link. The movement speed was about 40 km/h.

The most notable parameters for evaluating voice transmission are the Packet Delivery Ratio (PDR), the end-to-end delay and the variance of the voice packet inter-arrival time (jitter). The following sections show the result of the experiments.

PDR and MOS

Table 6.2 lists the main results related to the characteristics of the voice transmission obtained in the real experiments when the two mobile nodes were communicating with each other. PDR is a measure of the percentage of packets that reach the destination (see Section 1.4). In our tests, we registered values around 98%

during the whole duration of the test. With this level of PDR, speex audio codec guarantee a MOS greater than 3.5, which was approximately the MOS level that we achieved during the test. This value is considered $fair$ (imperfections can be perceived but the sound remains clear).

Delay and jitter

The IAT in the real experiment (see Figure 6.10) is quite similar to the one obtained in the indoor experiment even if we can notice a little widening of the distribution due to the presence of a little percentage of discarded packet (about 2% as anticipated earlier). The analisys of the same parameter as a function of the time presents also a similar behavior but again in a wider range due to the fact the nodes that were not in a virtual chain but were free of communicating among them following the routing algorithm based on real link quality.

Figure 6.11 shows the distribution of the end-to-end (from mouth-to-hear) delay obtained during the real experiment. Again, the shape is a little wider due to the movement of the node along the tunnel but conserve the behavior of the simulation experiments. The most part of packets were delivered within 100 ms of its creation, honouring comfortably its deadlines.

RSSI and Prim Based Routing

Figure 6.12, tries to illustrate the effectiveness of the Prim and RSSI based routing algorithm. As in figure 6.8, the red line shows which (backbone) node have delivered the message containing the voice data to the mobile node (node 0) and the link quality among them. As can be seen, at the beginning frames where directly exchanged between the mobile nodes 0 and 6 (due to the fact that they were close each other) or through node 5. When node 0 started to move towards the end of the backbone (node 1), the routing algorithm adapted itself to provide always a good delivery path. This is reflected by the fact that the last-hop was executed by different nodes during the movement along about 7.5 km of the tunnel.

The graph shows, despite the high level of noise that is usual in RSSI measurement, the good work of the routing algorithm specially thanks to the introduction of the Prim algorithm. In fact, it promotes the exchange of data among the mobile nodes and the closest (from the link quality point of view) *backbone* node. As can be seen, the RSSI is maintained above the value of $-60dBm$. This value is considered high enough to guarantee a reliable link.

Traffic Influence

The most part of the experiments have been carried out in an empty tunnel in which the only vehicle involved was the one that transported the mobile node. However, to verify the influence of the traffic on the communication, we carried out an additional experiment simulating the presence of a light traffic. We positioned

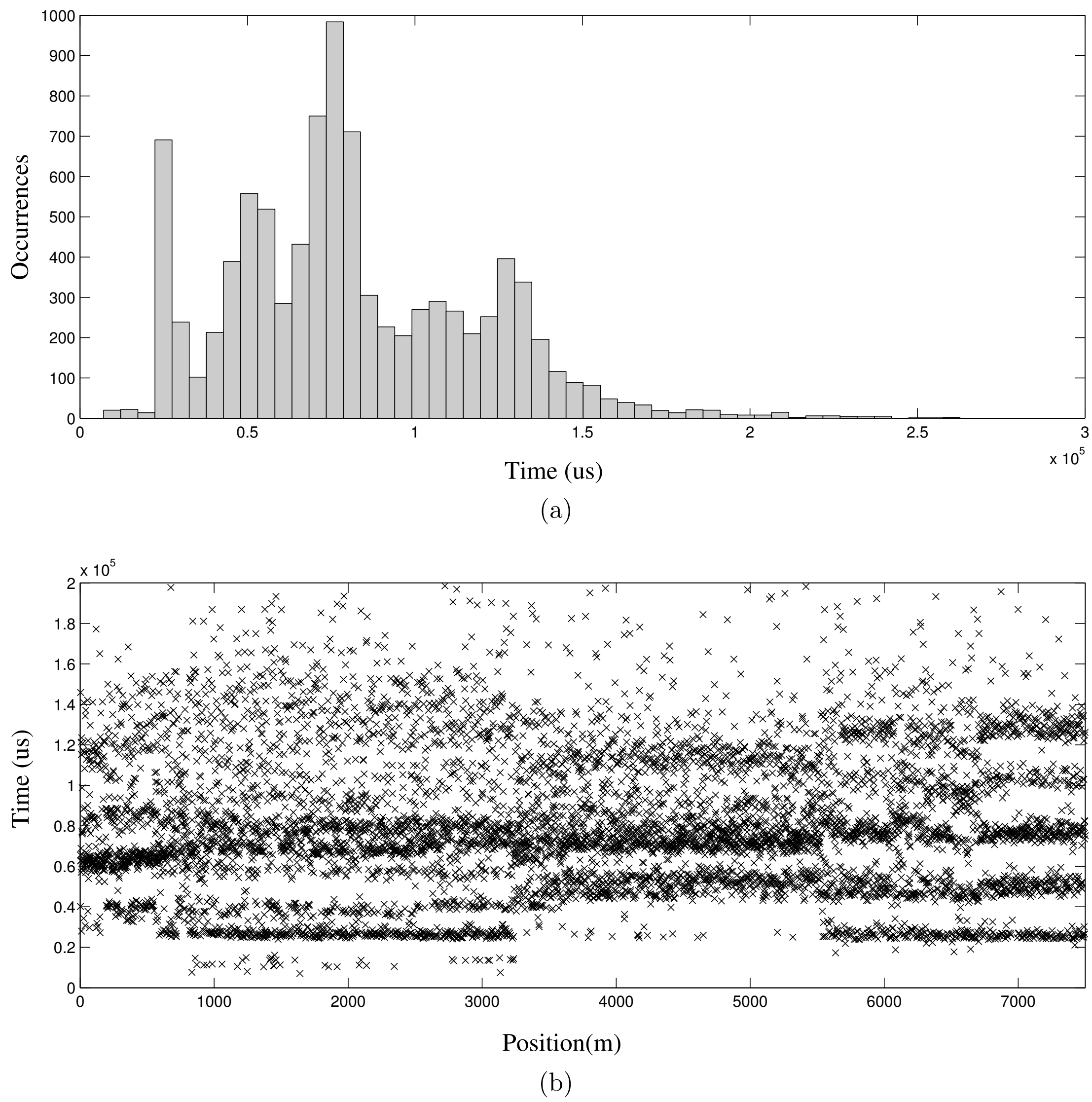


Figure 6.10: (a) Distribution and (b) raw data of Inter-Arrival Time (IAT) in the real experiment.

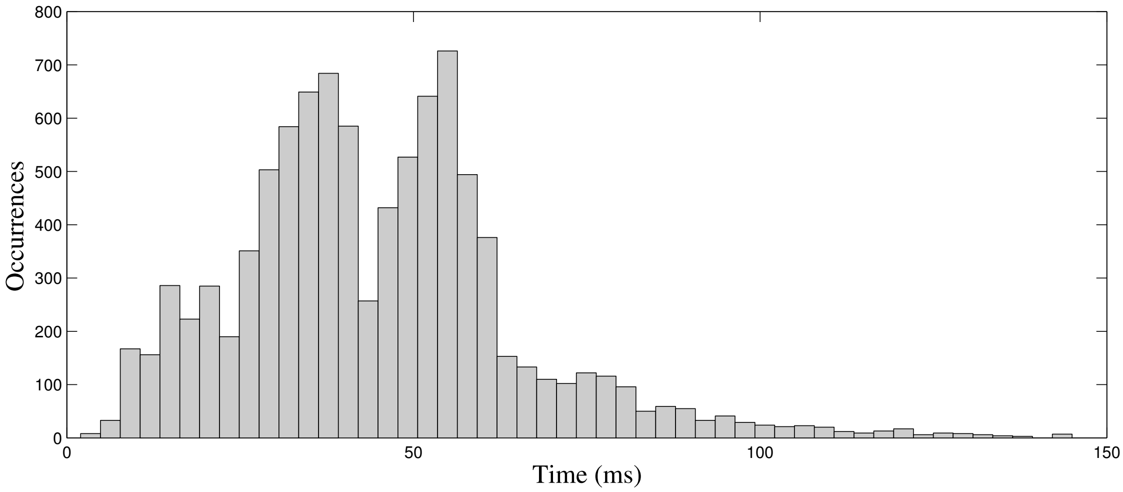


Figure 6.11: Distribution of end-to-end delays in the real experiment.

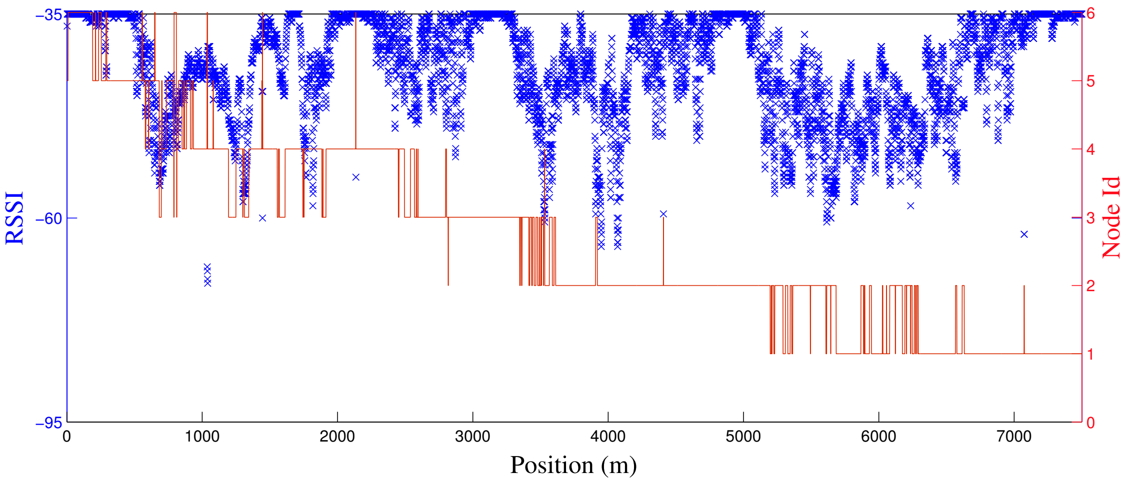


Figure 6.12: Identity of the node that delivered the data packet to the mobile node and the RSSI value with which destination node has received the frame.

two backbone nodes 1.2 km apart each other (with LoS among them) and generated a simulated voice flow. After recording in both nodes the frames exchanged during two minutes without obstacles, we sent a first car from the position of the first node to the the position of the second one at a speed of approximately 35 km/h. Successively two cars, few meters apart each other, traveled the same route at the same speed.

The cars never closed the LoS between that backbone nodes since the latters were positioned close to the tunnel wall. It is assumable since in a hypothetical permanent installation they would be secured on the top of the tunnel without possibility of losing LoS.

The data collected showed that, in this configuration, the traffic only has a little influence on the communication. The PDR fell from 99.86% in the obstacle free experiment to just 99.84% with one car and 99.832% with two cars.

6.1.5 Conclusions

This work addresses the problem of allowing multimedia QoS communication between mobile nodes in underground environments (tunnels, mines, etc.). The scheme proposes the deployment of a set of backbone nodes along the confined area that act as relay for QoS data that mobile nodes exchange during its movement. It is based on a complete software/hardware network architecture using low-cost commercial hardware and running the RT-WMP protocol and its QoS extension. Thereby, the latter has been specialized to take advantage of the a priori knowledge of the network topology.

The whole system was finally tested in the Somport tunnel at the presence of the tunnel crew, the director of the road unit of the Huesca province and representants of the Spanish Ministry of Public Works with satisfactory results, in August, 23, 2009 and again in July, 19, 2010.

The real experiments show that it is a valid, flexible and easy-to-setup solution for supporting QoS flows in tunnels, mines or disaster zones where the use of an infrastructure network is impossible or too expensive.

6.2 Robot teams for exploration in underground environments

In certain fields of application such as emergencies, battlefields or hostile environments, there is a growing interest in robot teams for surveillance, exploration or rescue missions. A typical application involves several robots with differents sensory capabilities which have to cooperate, interact with the environment and with humans. In a real experiment this means dealing with several topics such as motion control, cooperative navigation and perception, localization and communication. In addition, each of these issues has to take into account the specific environment characteristics.

In this kind of experiment, connectivity capabilities play an essential role. To cooperate, robots must exchange information about their own state and the environment. Humans and robots can be thus organized in a MANET to accomplish this requirement. These networks are usually multi-hop, that is, nodes also act as routers, to increase coverage and to deal with the changing network topology. Additionally, a MANET for robotic team applications must provide Real-Time traffic to exchange time-constraints data and connectivity guarantees. As it is well known, in fact, all control applications have strict real-time requirements. In distributed control applications, such as those of robotic teams, the requirements extend to communications. Moreover, human communication should use the same MANET as the robots, and the system must be able to support some class of QoS to allow voice communication, for example. In these situations the use of a real-time capable network is mandatory to allow distributed perception and prioritized information flows.

Despite the impact of communications, in the literature, communication and robotics issues are usually treated separately. In this section we treat to give a contribution in this sense, showing a case study that tries joining communication and robotics.

Specifically, we achived that combining four modules: a COMmunication module (COM), a Navigation Control Module (NCM), a LOcalization Module (LOM) and a SUpervisor Module (SUM). The COM module allows to achieve connectivity by means of a multi-hop communication network with real-time capabilities, maintaining end-to-end voice communication with QoS between the operator and the farthest mobile robot and allowing the operator to monitor any phase of experiments and, if any, manually control the robots.

This contribution was developed within the framework of the TESSEO Spanish National Project and the Roboearth European Project. The results were presented at the ROBOT2011 Workshop [Tardioli 11].

6.2.1 Related work

The use of teams of robots in dangerous or hostile environments have become interesting in the last year thanks to the fact that the technology is now mature enough to allow this type of application and (sadly) to the fact the it has been necessary to act in real applications in which the risk for human being was too much high. Already in 1986 in Chernobyl, telemanipulated robots were used to clean up the roof of the nuclear energy plant exploded in the famouse accidents. They failed due to the very high radiation level but it was one step toward the use of the robots in dangerous zones.

Various applications and projects involving safety in tunnels and using robots have been developed. These include robots for fire-fighting, exploration, inspection, sensor deployment or surveillance. For example, in [Suthakorn 09] the authors present the design and development of a single semi-autonomous robot for rescue missions controlled by a remote station. In [Walker 09] the authors describe a project involving a robot for surveillance in underground galleries against smugglers in national borders. The problem of the loss of communications is mentioned but no solutions are proposed. In [White 10], an underwater robot for archaeological teleoperated exploration in cisterns was presented. The work focused mainly on SLAM problems for mapping the cisterns whilst communication issues were not considered. In [Peasgood 06] a work about multi-robot path planning in tunnel-like scenarios is presented. However, only simulation results were shown, and the multi-robot communication problems were not addressed. In [Zhuang 08], a robot for inspecting tunnels, capturing images and registering the concentration of some poisonous gases was developed. Similar experiment, with regarding mine exploration, are presented in [Murphy 08] and [Yarkan 08]. In [Nguyen 04] the objective is to maintain communication between a robot and a base-station. To accomplish this goal, a set of relay robots follow the lead robot. In [Tanabe 11] an application for sensor networks deployment in underground scenarios by means of one robot was proposed. The teleoperated robot was able to deploy devices to ensure, restore or extend the communications, taking into account the RSSI of the signal among them.

All of these cited works were focused on single robots, on their mechanical aspects, on mapping and on specific applications, without considering the connectivity problems.

6.2.2 Overview

In this work we present an experiment that tries to simulate an accident scenario in a long tunnel and were no human-beings can access to verify the situation due to the dangerous conditions (gas, fire, etc.). The scenario is the Somport tunnel, described in the section 5.3. The idea is to explore the tunnel using a team of mobile robots equipped with different sensors. The goal is to reach a shelter where there is an injured person, establish a vocal and visual communication with him/her to decide a rescue plan or to calm him/her down until the situation allows the missions of the firemen.

For this experiment we chose a part of the tunnel between the 13th and 14th lateral galleries. The room at the end of the latter was selected to be the location of the injured person (point "c", in figure 6.13). This is a fully equipped emergency shelter where people can take refuge in event of accident or fire in the road tunnel. A base station was established about 300 m apart from the cross between the lateral gallery and the tunnel itself (point "a" in figure 6.13). The idea was to reach the lateral gallery (point "b" in figure 6.13) and then the shelter, explore it by means of laser range sensor, and camera (mounted on top of a pan-tilt mechanism) telemanipulating the robot and finally establish a full-duplex voice communication with the injured person.

Experiment size makes each pair of nodes experiences a longitudinal variation of the signal of the "Near Sector" described in Section 5.3.3. In this sector, distance path loss dominate and the fast-fading effect results tolerable, due to the RSSi asumes values above of the -60 dBm level (see Figure 5.4).

However, the considerable distance and, above all, the absence of line of sight between the base station and the presumed robot in the shelter, do not allow the direct communication between them, considering the limited range and power of the commercial 802.11 cards used. The solution was to use two robots, one of which had the task of acting as a relay between the head robot and the base station.

6.2.3 Details of the plan

The two robots, named $R1$ and $R2$ start their deployment together (but in chain) from the base station BS and towards the intersection point at a costant speed (about 0.8 m/s). They were using a laser-segmentation-based localization algorithm and using a pre-existent map. The head robot $R2$ had a *global goal* at intersection between the lateral gallery and the tunnel itself. However the local navigation was completely reactive and based in a modified version of the Nearness Diagram (ND) algorithm (see section 6.2.6 for details). The robot $R1$ followed the leader at a distance of about 7 meters. A goal at that distance behind the leader was continuously assigned to the follower that localized the latter by means of its own laser sensor.

The communication was based in the RT-WMP that, as explained in Chapter 2, supports multi-hop and message priority allowing the exchange of information among the three nodes with efficency and flexibility (see section 6.3.4).

When $R1$ and $R2$ reached the intesection point (figure 6.13.b), $R2$ and thus $R1$ stopped few meters apart each other. After that, a goal within the shelter was assigned to $R2$ while a command to keep that position was sent to $R1$. Robot $R2$ started to move while $R1$ was acting as a relay to allow the communication with the base station. The leader robot continued correctly localized until the door of

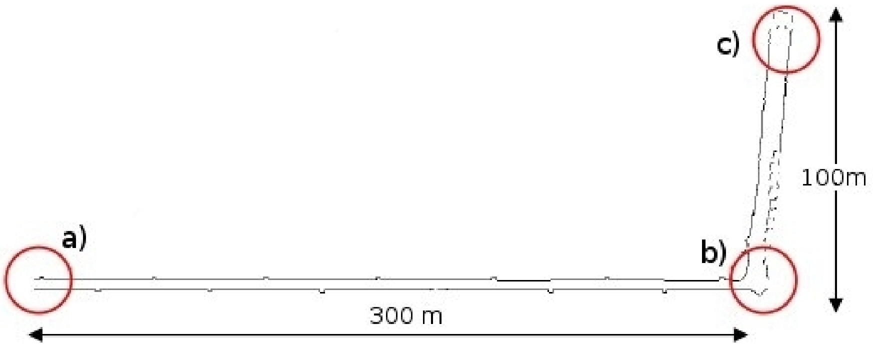


Figure 6.13: Map of the portion of the tunnel used in the experiment.

the shelter. Afterwards it was opened by the injured person and the robot reached its goal within the shelter.

All the process was supervised by an operator at the base station which could see, by means of a specific graphic user interface (GUI), the laser readings of the robots and the link quality among them and with the base station. Once $R2$ reached its destination, the operator started the manual control of the robot to explore the shelter. Using a joystick, it was moved through the room helped by a frequent laser feedback.

During the exploration, the operator could move the pan-tilt mechanism (again using the joystick), and obtain snapshots of the environment from the camera. All the flows - laser readings, joystick commands, camera snapshot and robot control command - travelled as real-time RT-WMP flows with different priority.

Once localized the injured person, a voice communication was established by the operator. One full-duplex 30 Kbps speex-coded [RFC5574 09] flow (2 flows of 15 Kbps each one) was managed by the QoS extension of the RT-WMP protocol [Sicignano 10b]. After a short communication, it was time for the robots to go back. A command requested by the operator at the base station provoked $R1$ to turn 180 degrees and $R2$ to start going towards the base station. Since both $R1$ have the goal of following the lead robot, it started following $R2$ when the latter entered in its field of view, that is, when it was overtaken and was 7 m ahead. Both $R1$ and $R2$ reached the base station. At this point the mission was completed.

6.2.4 Hardware and Software Architecture

This section presents the hardware and software architecture used in this experiment. In order to perform tasks in hostile conditions, each of the robots must have a basic structure that allows it to navigate autonomously in complex environments. They also have to incorporate a system that allows communication with a base station where a user can send commands in order to control the robots.

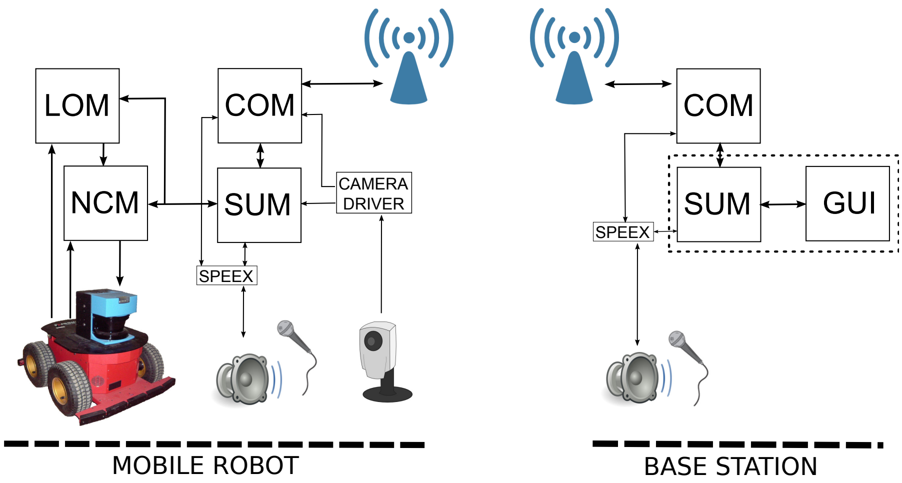


Figure 6.14: Modules and information flows.

Hardware architecture

For this experiment, we have used a team of robots composed of two Pioneer P3-AT robots (ActivMedia MobileRobots). Each robot is equipped with an on-board PC with a Pentium III processor at 800 MHz. Regarding the wireless communications, the robots have an Atheros 802.11 a/b/g wireless card in order to exchange information between them and the base station, and for monitoring the quality of the signal between them. Depending on the role that has the robot in the team, it will incorporate differents sensors. The only common sensor for all robots is the laser sensor. The robot incorporates a SICK LMS 2000 laser range finder. This sensor gives us the ability to configure their maximum range up to to 80 meters. This feature is very useful, since in the experimental environment we work with great distances. The robot that has to go inside the shelter incorporates a microphone and a speaker in order to establish a communication with the base station. It also has a camera (Unibrain Fire-i) to capture images.

Finally, the base station consists of a laptop with an Intel Core 2 Duo 1.6 GHz processor and an Ubiquity 802.11 a/b/g wireless card. The base station also has a speaker and a microphone to communicate with the leader robot and the injured person and a joystick to control remotely the robots and the pan/tilt mechanism.

Software architecture

The software architecture was implemented over the onboard computers which run a Linux Debian with kernel 2.6.18. It has been designed and implemented in a modular solution replicated in each robot (figure 6.14):

- The COM module provides multi-hop, real-time communication among robots and base station. It also measures the communication link qualities among robots and base station. Additionally it offers QoS communication between the lead robot and the base station.

- The NCM module generates velocity commands for the robots, providing a safety navigation towards the goals assigned by the SUM. It uses the information of the robots' sensors (odometry and laser) combined with the localization provided by the LOM module, in order to carry the navigation out.
- The LOM module provides a global localization for the robots, using the information of the laser and odometry sensors and a pre-existent map. This localization information is also sent to the SUM module that exports it to the COM module that, in turn, send it through the network to the base station.
- On the robot side, the SUM module is in charge of sending commands to the other modules (goals, emergency stops, resumes, etc.) and is also responsible for selecting the flow of information to send through the network (e.g. laser readings or voice). On the base-station side, it generates such commands, once requested by the operator through its GUI.

The remaining modules (speex and camera driver) shown in the figure 6.14, are auxiliary modules used to access to the multimedia devices.

6.2.5 Communication Module

As anticipated, the communication among the robots and between them and the base station must obey to a set of important conditions and characteristics. Above all, the network protocol must support multi-hop communication since is not possible a direct connection between the lead robot and the base station, due either to the excessive distance and to the absence of the line-of-sight between the two ends. On the other hand end-to-end delay must be known and bounded: joystick commands, for example, must reach the robot with few delay to allow a correct telemanipulation. We can say the same for the laser data that must be visualized frequently to give a useful visual feedback. Also, message prioritization is fundamental since, again, laser data must have priority over, for example, image data and joystick commands over laser to avoid dangerous delays in the control. Finally network must be able to support Quality of Service (Qos) traffic to allow the transport of voice.

The RT-WMP and its QoS extension, described in Chapter4, offer all of these characteristics together.

6.2.6 Navigation Module

The navigation module is composed of two layers. The low-level layer which is in charge of providing a safe navigation, and the high-level layer that provides the tasks to the robot. Given a goal, the low-level layer is able to provide a safe navigation in order to reach it. This module ensures that, regardless of who assigns the goals (high-level layer or the operator at the base station), the robot can navigate safely to them. A new method called Nearness Diagram High Speed (ND-HS) is carried out by the low-level navigation layer: it combines the ability of the obstacle avoidance method ND [Minguez 04] to navigate in dense environments with that to navigate at higher speeds when there are no obstacles nearby. In the figure 6.15 an outline of the technique used is shown.

The second component is the high-level layer, which is in charge of assigning to each of the robots their target. These targets may change depending on the role of the robot and the phase of the experiment in which they are. Three navigationmodo exist. The first mode is to go to a target, sending to the low-level layer all the goals that come from the SUM layer. The second oneis the telemanipulationusing a jostick The third mode, tracking mode configuration, allows moving a chain of robots where each of them follow the preceding one when the leader moves.

More details are present in [Tardioli 11].

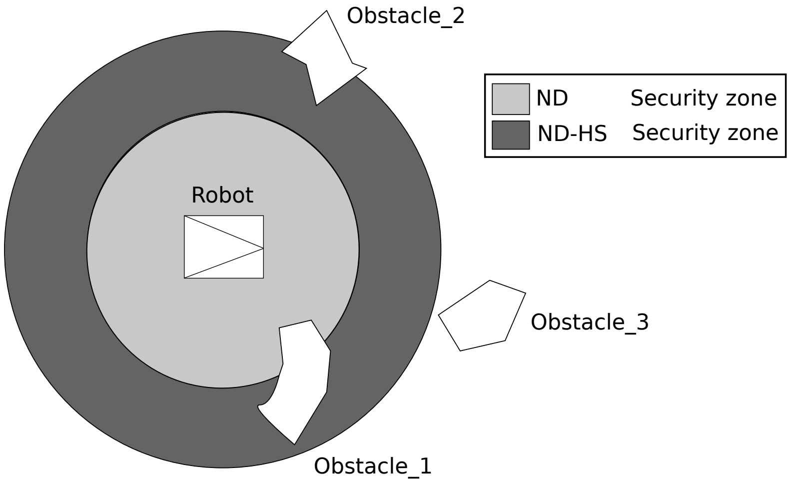


Figure 6.15: Diagram of the security zones of the algorithm.

6.2.7 Localization Module

The localization module provides the robot position using a two-dimensional map and information extracted from the laser readings. Starting from a map of points, it has been segmented offline and all the features have been stored in a segments-set that describes the environment. When online, the localization algorithm segments the laser sensor readings and tries to match the features obtained with the set of those representing the map. The laser sensor segmentation technique is based on a tracking-like algorithm combined with a validation gate used to classify the range readings into regions. These regions are successively splitted into segments, which approximate the environment seen by the robot, through a polygonal approximation technique. These observations are matched with the map features to decrease the location uncertaintity of the robot and then are combined with the predicted location that comes from encoders using an Extended Kalman Filter (see [Castellanos 99] for details).

6.2.8 Supervisor Module

A pratical issue in a robotic surveillance experiments is the direct control of all the phases of the mission. The SUM module is the software component in charge of providing the supervision of the events that take place during the mission. The SUM has two different identities that resides in two different places: the robot-side and the base-station-side. On one hand, the base-station-side is in charge of sending, through the COM, the command generated by the operator at the GUI. Such commands are:

- *Start, return and abort mission command*: it initialyzes the formation to start the mission and to send the return command. It also allows to abort the mission if a problem occurs.
- *Goal selection*: the GUI provides a point-and-click utility to select the a global goal in an easy way.
- *Telemanipulation control*: By moving the joystick, a goal is assigned to the navigation algorithm as a function of the stick position for telemanipulation actions.
- *Pan-tilt control*: it provides an interface to control the pan-tilt of the camera using a jostick.
- *Photo request*: by pressing a button, there provides users a fast way to capture a single environmental image.
- *Laser readings request*: the function requires the laser readings to a specific robot.
- *Voice communication request*: this feature enables voice transmission between the base station and the last robot.

All the commands are sent through the COM using the *command* flow and act directly on the robot-side SUM. Some of that are request-reply commands (e.g. photo request) while other only act on the correspondent module (e.g. telemanipulation control). Finally two of them, *voice communication request* and *laser request*, activate a service that offer laser views of a specific robot and voice link with the leader robot respectively.

The GUI is in charge also of interpreting, visualizing or reproducing the input information flows (laser, photos, etc.) and offers:

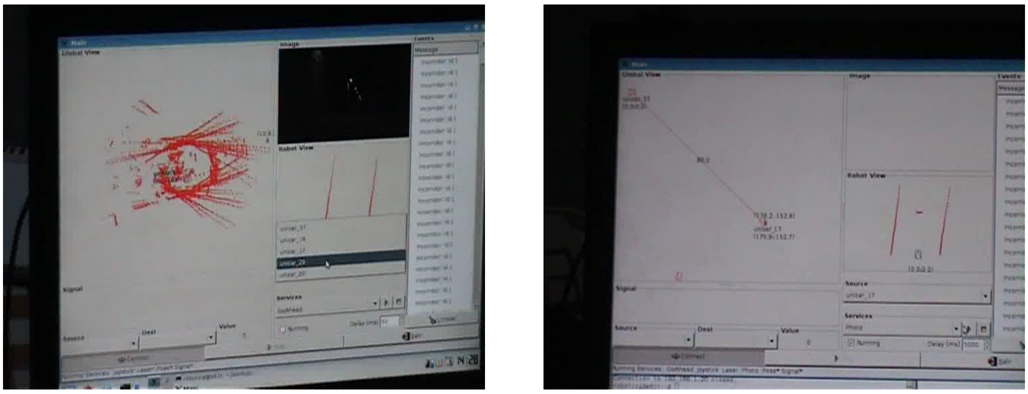


Figure 6.16: Two snapshots of a laptop screen running the GUI in the base station.

- *Global map visualization*: a global vision of the environment is offered in a main view to localize robots at all times.
- *Robot laser readings*: the function shows the actual laser scanning in a specific view.
- *Photo visualization*: the photo received from the selected robot (after a specific request) are visualized in a image view.
- *Voice record/play*: encode/decode and replay voice from/to the leader robot.
- *Link quality check* Operators can check constantly the link quality between robots and the base station.

Two snapshot of the GUI are showed in figure 6.16.

On the robot-side, the SUM is in charge of executing the commands sent by the operator activating the voice service or sending a goal to the NCM module, for example, when requested. It also sends autonomously the localization to the base station requesting it to the LOM.

6.2.9 System network configuration

As anticipated, several flows of information both real-time and QoS were involved in the communication. Globally we used 6 real-time flows and 2 QoS flows.

Specialization on the environment

Although RT-WMP has been designed to support real-time communication giving support to any type of topology, in thes experiment considered here, most of the time the three nodes will constitute a chain network. We used this a priori information to improve the routing adding a Prim-algorithm based scheme in a similar way as we presented in Section 6.1.2.

Name	Size (B)	Frequency (Hz)	Priority
Joystick	8	on-demand	5
Robot Control	8	on-demand	4
Pose	16	10	3
Laser	720	4	3
Pan-tilt	8	on-demand	2
Camera	$1.5K$	on-demand	1

Table 6.3: Real-time flows used in the system.

Real-time flows

Table 6.3 shows the characteristic of each flows. The most part of the flows are on-demand. Only the poses and the laser scans are updated with a constant frequency but, while the two robots update their poses simoultaneously (2 identical flows towards the base station) to allow a more useful visualization in the GUI, the activation of the latter flow is requested by the base station to reduce the bandwidth needed by this task.

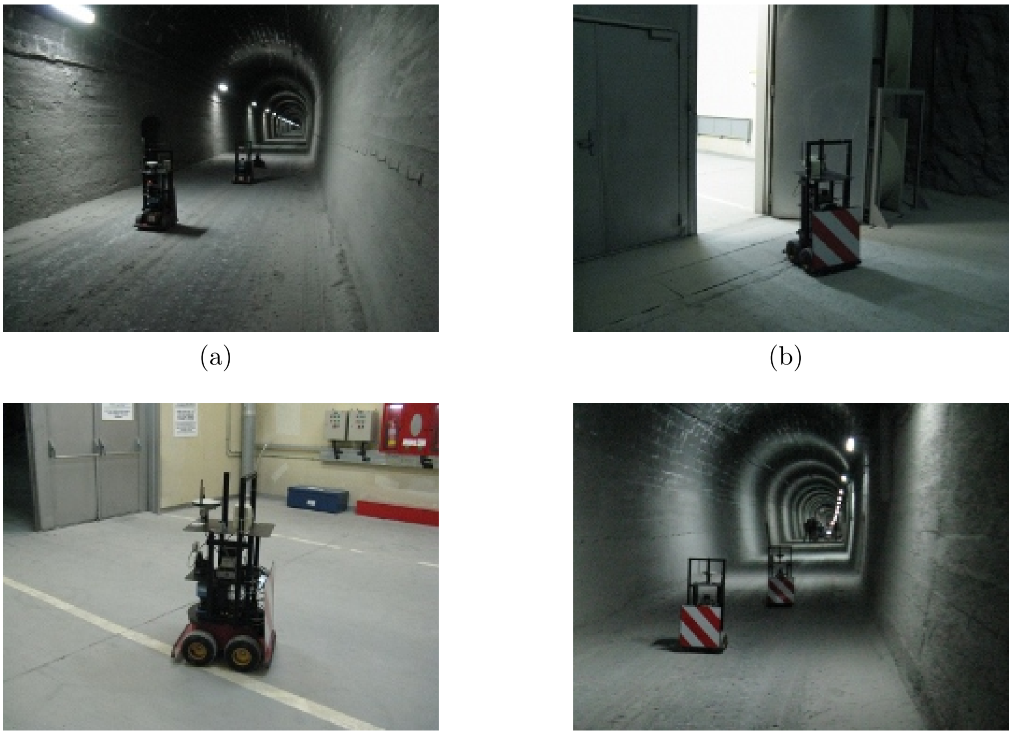
The *robot control* flow, originated from the SUM, is in charge of managing the robot in particular situations (for example an emergency stop) or to give specific commands to the robot (to force a relocalization, for example) or, again, to select which robot has to send its laser scan over the network.

The joystick-command messages, also originated from the SUM are sent after a joystick movement and have the highest priority for the reasons discussed earlier.

The camera-related flows (pan-tilt and images) are considered the less critical. Thus they have the less priority. Especially the image flow is the less priority of the system. In fact, even if the snapshot captured by the camera is resized and compressed to obtain a *jpeg* format, it normally has a size of about 3.5-4 KB (320×200 pixels, black and white format). Since the biggest message that the RT-WMP can manage is 1500 bytes, the image has to be split in three parts that are sent separately in different RT-WMP loops. If their priority would be high, it could delay more important flows like joystick commands.

QoS flows

The two QoS flows have identical requisites. The objective is to have good-quality full duplex communication with as less as possible mouth-to-ear delay. To obtain a continuous flow without cuts or interruption, voice packet must be exchanged among mobile nodes with and adequate frequency and within its deadline. It means that if the protocol is able to deliver a message each 50 ms, for example, such a message must contain *at least* 50 ms of voice. The worst-case Inter-Arrival Time (IAT) (see [Sicignano 11]) that the communication network is able to offer in a 3 node chain configuration is about 50 ms. Since that the *speex* codec [RFC5574 09]



(a) (b) (c) (d)

Figure 6.17: Screenshots from real experiment. We can see the formation moves along the tunnel (a), how the last robot approaches (b) and explores the shelter (c) and finally formation coming back to initial point(d).

used in the communication generates data packets containing 20 ms of voice each one, we need to send at least:

$$n_{samples} = \left\lceil \frac{50}{20} \right\rceil = 3 \tag{6.6}$$

samples (60 ms of voice) in any loop. On the other hand to absorbe sporadic high-IATs, we set a reception queue q of 3 packets considering an IAT_{max} of

$$IAT_{max} = q_{size} \cdot 20ms \cdot n_{samples} = 3 \cdot 20 \cdot 3 = 180ms \tag{6.7}$$

The IAT_{max} also represents the delay added by the queue to the mouth-to-hear end-to-end delay of the packets. This value is however assumable as guaranteed by the ITU-T recomendations [ITU-T 03]. On the other hand the packets' deadline was fixed at 150 ms that correspond to maximum end-to-end delay admitted for multimedia traffic [Vlaovic 01].

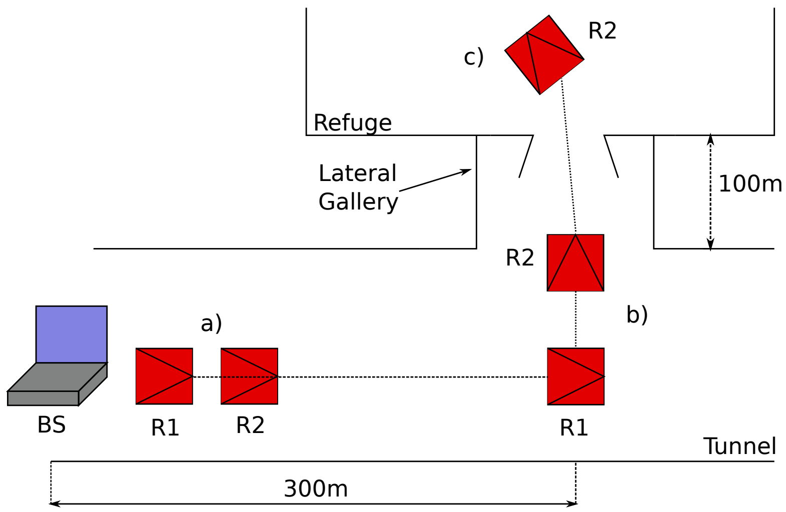


Figure 6.18: Phases of the experiments (way out).

6.2.10 Results of the experiment

In this section the results of the experiment described in section 6.2.2, successfully carried out in the Somport tunnel are presented. Figure 6.17 shows some moments of the experiment. Additional videos are available at [Multimedia 11].

The formation starts in its initial configuration close the base station. The start-mission command is sent through the GUI and the formation moves along tunnel maintaining a stable trajectory, how shown in figure 6.17a.

Figure 6.17b shows how the last robot $R2$ approaches the shelter. The exploration of the shelter is instead showed in figure 6.17c. Finally, as a result of a command requested by the operator, the robots return to the base station (figure 6.17d).

Communications

The bandwidth consumed in static conditions by the real-time flows was about 25 kbps with peaks of 70 kbps when had to manage an image request. Considering that we configured the wireless device to a rate of 11 Mbps, the RT-WMP had no problem to manage this flow of data even in presence of QoS flows that occupied globally 30 kbps.

On the other hand, it is interesting to analyze the quality of the links between the three nodes during the experiment. Figure 6.18 shows the relevant phases of the way out and figure 6.19, the link qualities in terms of Received Signal Strength Indicator (RSSI) between the base station (BS), the head robot ($R2$) and its follower ($R1$). At the beginning the three nodes are close each other and the signal among them is about 100% (figure 6.18.a). Then $R1$ and $R2$ start to move: the RSSI between them is more or less constant (despite the noise) and stays around

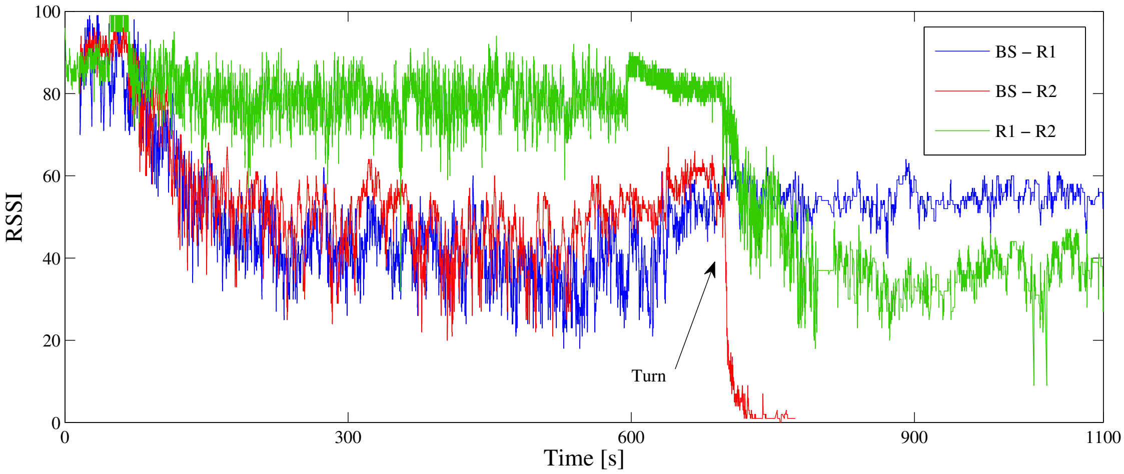


Figure 6.19: RSSI among robots and base station during the way out.

90% (they are only few meters apart). However the signal between them and the base station starts to fall, as expected, due to the increasing distance. When the robots are close to the intersection point, $R1$ stops while $R2$ enters the lateral gallery (figure 6.18.b). Suddenly a strong link quality fall affects the link between BS and $R2$ due to the loss of the line of sight between them. Also the link quality between $R1$ and $R2$ suffer from a fall but it is smoother and stabilizes at about 30% even when the robot $R2$ enters and stay within the shelter (figure 6.18.c). On the contrary the link between BS and $R1$ remains in optimal values during the whole experiment thanks to the good propagation characteristics of the tunnel that, at the frequency used (2.4 GHz), acts like a waveguide.

The connection between $R2$ and the base station has been maintained during the whole experiment (see Figure 6.19). The use of the Prim-based specialization helped to maintain a very low percentage of errors in terms of RT-WMP packet loss (about 1.12%) since nodes always used the best links to communicate.

From the point of view of the QoS traffic, we have considered the quality perceived by the user or MOS (see Section 1.4). Voice communication obtained a MOS of 3.5 approximately that is considered fair (imperfection can be perceived but the sound remains clear), being the QoS PDR higher than 96% for both flows. The mouth-to-ear delay was completly aceptable and did not bother the interlocutors.

The main communication results of the testbed are resumed in Table 6.4.

Dynamic

Figure 6.20 shows the velocities (linear and angular) of the lead robot during the way out. The linear speed was fixed at about 0.8 m/s. However it suffered from many oscillations due to the uneveness of the ground that was full of small stones

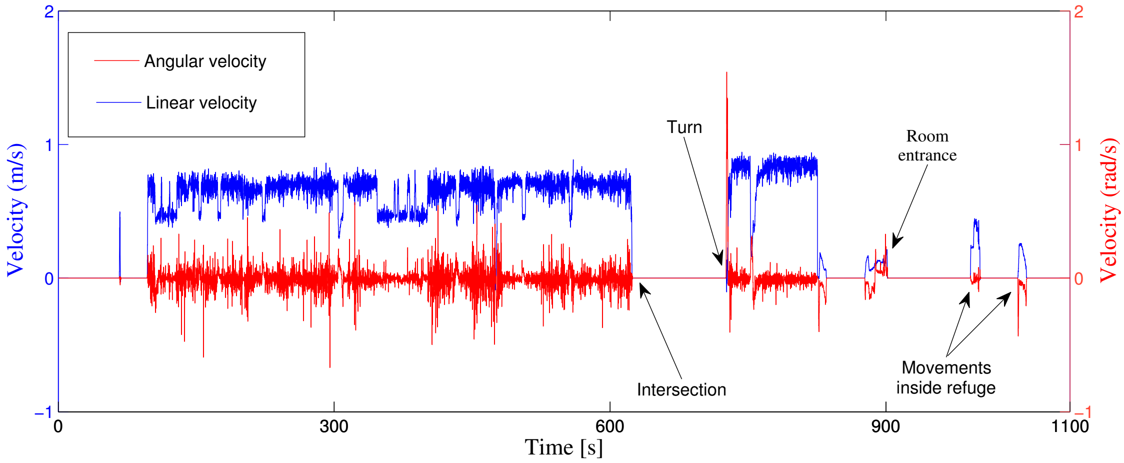


Figure 6.20: Velocities of the lead robot during the way out

and pot holes. The same irregularities provoked a frequent reorientation of the robot, also visible in the graph showing the angular velocity. The graph, moreover, shows clearly the moment in which the robot reaches the intersection point (arount point 620 s) and when it, after an abrupt turn, starts to travel toward the shelter in the lateral gallery. In this second stretch, the velocity was slightly higher thanks to the fact that the gallery is a little downhill.

Once the robot reached the door, it reduced the speed to enter the shelter guided by the reactive navigation algorithm. When inside, the operator moved manually the robot causing visible changes in the linear and angular velocities.

	RT-WMP	**Flow 1**	**Flow 2**
Pkt Loss	1.12%		
PDR [%]		96.11 %	96.9 %
MOS		≥ 3.5	≥ 3.5

Table 6.4: Main testbed results.

6.2.11 Conclusions

In this work we presented the results of an experiment whose objective was to explore in a semi-autonomous manner an emergency shelter where a presumed injured person is waiting for assistence after an accident. During the experiment, carried out in the Somport tunnel, a team of two robots was sent toward the shelter situated in a lateral gallery of the tunnel about 400 meters apart, while a human operator supervised the operations in a base station by means of laser-scan and camera feedbacks. Once one of the robots arrived at the shelter the operator could move it using a joystick and interact vocally with the injured person.

The system has been structured in different interacting modules where the communication task played a critical role.

The analisys of the results shows the need for a multi-hop communication, carried out by the RT-WMP protocol, since the direct communication between the lead robot and the base station was not possible due to the excessive distance and to the absence of line of sight. Moreover, end-to-end voice communications was supported by the QoS extention. On the other hand the results show the effectiveness of the localization, the navigation and the supervisor algorithm.

6.3 Signal based deployment planning for robot teams in fading environments

Deploying a multi-robot team in confined environments poses multiple challenges that involve task and motion planning, localization and mapping, safe navigation, coordination of robots and specially the connectivity among all of them.

Dealing with connectivity issues has become a real necessity as real applications are developed. Initially, simple theoretical propagation models in which only the distance to the source was considered were used. However, in the real world such simple models do not work well because scenarios may be complex or dense, or may contain obstacles. Furthermore, the propagation of the signal may involve particular difficulties.

The main contribution of the present work is that proposes a technique for deploying a multi-robot team in tunnel-like fading environments while continuously maintaining the network connectivity, taking into account the intrinsic signal-propagation behavior. To the best of our knowledge, multi-robot deployment profiting from the signal transmission characteristics in real and large fading environments has not been addressed.

The technique uses parameters obteined by the signal propagation analysis described in the Chapeter 5 to drive the deployment. The complete system involving all the above-mentioned robotics tasks has been evaluated by means of simulation and in a real scenario.

This contribution was developed within the framework of the TESSEO and TELOMAN Spanish National Projects. The results will be pubblished in the special issues on Robotic Communications and Collaboration in Complex Environments of the International Journal of Robotics Reserch (IJRR) [Rizzo 13].

6.3.1 Related work

Control the motion of a team of robots to accomplish a mission objectives while maintaining network connectivity is a fundamental issue that has been received little attention in the robotic literature. That is especially true for applications involving robotic missions in real scenarios and many problems remain unsolved, especially in confined areas.

In previous works, signal propagation analysis was used for robot team exploration and missions in urban scenarios. In [Hsieh 08], a system to maintain connectivity of a robot team is described. A signal map is previously constructed to be used subsequently for the exploration strategies in urban environments. From the signal map, a roadmap connecting areas to be explored is generated, and afterwards used to drive the team to designated targets. A reactive strategy, based on the measured signal strength and on a controller that computes actions from a potential function modeling the radio propagation is applied to maintain the link quality when the robots are deployed. A chain multi-hop network is created in the experiments. The robots have to move forward and backward to maintain the signal strength above the minimum acceptable level. In [Tardioli 10], the authors developed a system to deploy robots which simultaneously achieve mission tasks and maintain connectivity, also in urban environments. A task allocation technique constrained by the signal strength was also described. In that work, the system reactively constrained the motions of the robots depending on the measured signal to maintain the connectivity at all moment. In [Fink 10], methods are proposed for modeling and mapping radio signal strength with robots. A maximum likelihood estimation of the source location is provided and a robot-motion control-law is applied to localize the source. Experiments in an indoor laboratory and in an open area are described. A similar approach is described in [Wadhwa 11], where the authors improve the characterization of the spatial variations of the Received Signal Strength (RSS) over space using Ray Tracing. They propose an adaptive algorithm which uses RSS averages (short and long term) to estimate both the travelling direction towards the source, and how to proceed along the chosen direction. In [Yan 12], the authors developed communication-oriented metrics for optimizing the positioning of robot formations and use them as router to extend the coverage in fading environments. The authors use an objective function based on BER in a probabilistic framework under communication power constraints. The method improves the performance of other methods based on disc models, although it was only evaluated in a preliminary experiment in a small scenario.

However, how we said in the Chapter 5, electromagnetic waves do not propagate in tunnels as in those scenarios nor in free space, even if LoS is maintained between emitter and receiver. Thus, taking into account the fading phenomena and the inability to predict with sufficient precision the position or magnitude of a fading, the deployment of a tunnel application cannot be based only on a theoretical model. This difference poses other challenges for robot deployment planning which are addressed in this work.

Unlike the previous works based on reactive motion-control discussed in this section as, for instance, [Hsieh 08] and [Yan 12], this work presents a deployment strategy in fading environments that takes advantage of a previously built model, but that is able to react according to actual real-time measurements maintaining continuously network connectivity. In [Hsieh 08] a chain-based topology is arranged in a non-fading environment, where a reactive control based on a previously built signal-map and on signal measurements is applied to maintain an acceptable signal quality. The model-based technique of our proposal allows us to benefit from the signal transmission behavior identified in tunnel-like fading environments to reach the farthest location from the base station maintaining the network topologically connected at all moment. This is not possible with approaches that do not take into account the signal behavior. In [Yan 12] a probabilistic framework for both fading and non-fading environments is developed. A reactive motion control based on the optimization of an objective function (which describes transmission errors) is proposed and evaluated by means of a real experiment. The method looks for near locations within a window around the current mobile-robot pose, in which this function presents a maximum. The method does not guarantee the continuous maintenance of communication during the movement of the robots to their optimal positions. Moreover, it is applied only to a single fixed transmitter and to one mobile robot, used as a receiver in a preliminary real experiment.

The work is organized as follows. First, taking into account the signal transmission analysis of the Chapter 5, a deploying strategy for a team of robots is presented in Section 6.3.2. In section 6.3.3 we introduce the architecture of the system used to validate the latter. Finally, in Section 6.3.8 the method is evaluated both by means of simulation and a real experiment carried out in the Somport tunnel. Section 6.3.9 summarizes the main conclusions.

6.3.2 Deployment Planning

In this section we present a planning algorithm for the deployment of a robot team in a fading environment as a tunnel. In the previous section we characterized the signal propagation in a such kind of environment. The planning proposed here tries to exploit that characterization to establish a general strategy for planning the motion of the robots in this scenario. Two main objectives are pursued simultaneously:

- to explore the tunnel maintaining always the connectivity of the network formed by the robots and the Base Station (BS).
- to maximize the distance to be explored with the available robots.

Using the measured signal presented in the previous section, we could build off-line a deployment plan which reached the maximum distance computed from the model without loss of connectivity. But since the real signal might exhibit changes (although not very relevant as shown in Section 5.3.3) it is not possible to ensure that the connectivity will not be lost. Therefore, we claim that the deployment has to use the real signal measurement for driving the motion in real time.

Even so, the general propagation behavior obtained in the signal analysis allows the definition of a general strategy, that we present in this work. The performed analysis permitted to establish, apart from the *distance path loss*, two main components in the signal, the *slow-fadings* and the *fast-fadings*. Both pieces of information will be used in the algorithm. The most important aspect to consider in the strategy is how to cross the fadings without losing communication with the base station. For this, a robot called *leader* will use one or more robots as relays to explore fadings. The more challenging fading are the slow ones that appear in the *far sector* (see Figure 5.4) of a tunnel because its width and depth. The information about the fast-fadings will be used to tolerate them when appear having a RSSI under a selected *threshold* (see next paragraph).

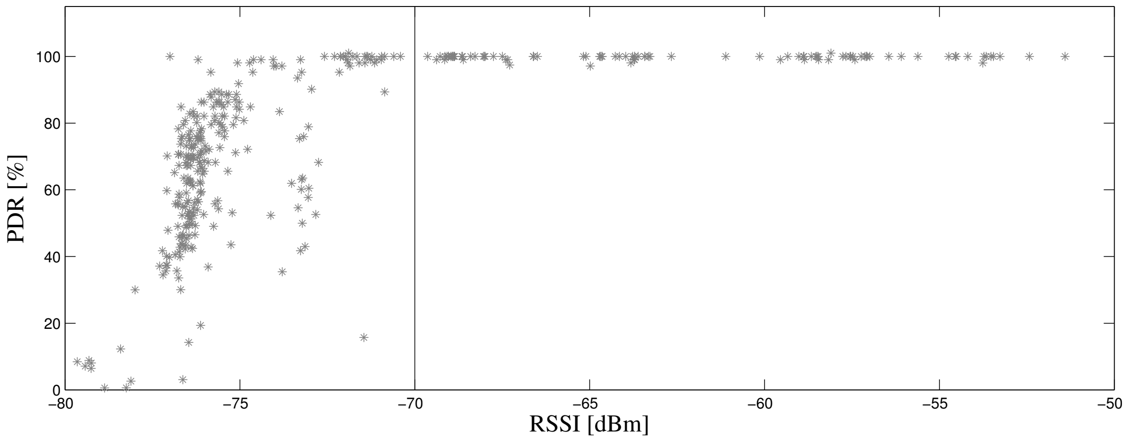


Figure 6.21: PDR vs RSSI. The line denotes the minimum Threshold chosen to ensure the acceptable PDR level.

The general strategy is the following: the leader continuously measures the RSSI with the BS. This information and the above mentioned parameters are used by the system to establish the subgoals for the follower robots, in such a way that always exists connectivity with the BS. When the leader is exploring a fading zone of the BS signal and do not find a new zone above the threshold, a new $base_i$ is set, being i the robot R_i closest to the old $base$. From this state, the plan restarts taking $base_i$ as new $base$. Notice that the maximum exploration distance for a fading will be the distance between two consecutive slow-fading. This distance can be computed from the measured signal that has been presented in Section 5.3.3.

RSSI threshold selection

How we stated in Section 5.2.1, at low rate a correlation between the RSSI and the PDR exists. In order to characterize this correlation with the hardware setup considered in this work, we consider the study performed in the Section 5.3.1, considering the PDR versus RSSI values for the 6Mbps transmission rate. The final goal was to establish the RSSI threshold that allows a reliable communication between the nodes, with no packet loss. The resulting threshold will be an important parameter that drastically condition the robot deployment plan. To this end, measurements were performed in several points, in order to obtain the PDR for a large range of RSSI. A scatter plot where is possible to observe the cited correlation between the RSSI and the PDR of the experiment is shown in Figure 6.21. It can be noticed that in order to obtain a PDR of 100%, the RSSI should be higher than -70 dBm. This will be selected as the threshold to avoid packet loss between nodes.

PARAMETER	DESCRIPTION	VALUE
Safe RSSI Threshold (TH)	RSSI value for PDR=100%	-70 dBm
Safe Distance (SD)	Maximum distance between two adjacent robots to ensure a link above TH	350 meters
Fast-Fading Width (FFW)	Fast-fadings found within this width are not considered	20 meters
Maximum Fading Distance (MFD)	Maximum distance between two consecutive slow-fadings	500 meters
Last Peak Distance (LPD)	Distance from a base to last peak above TH	2700 meters
First Valley Distance (FVD)	Distance from a base to the first fading below TH	1000 meters
Maximum Distance (MD)	Maximum exploration distance	N*LPD+FVD meters

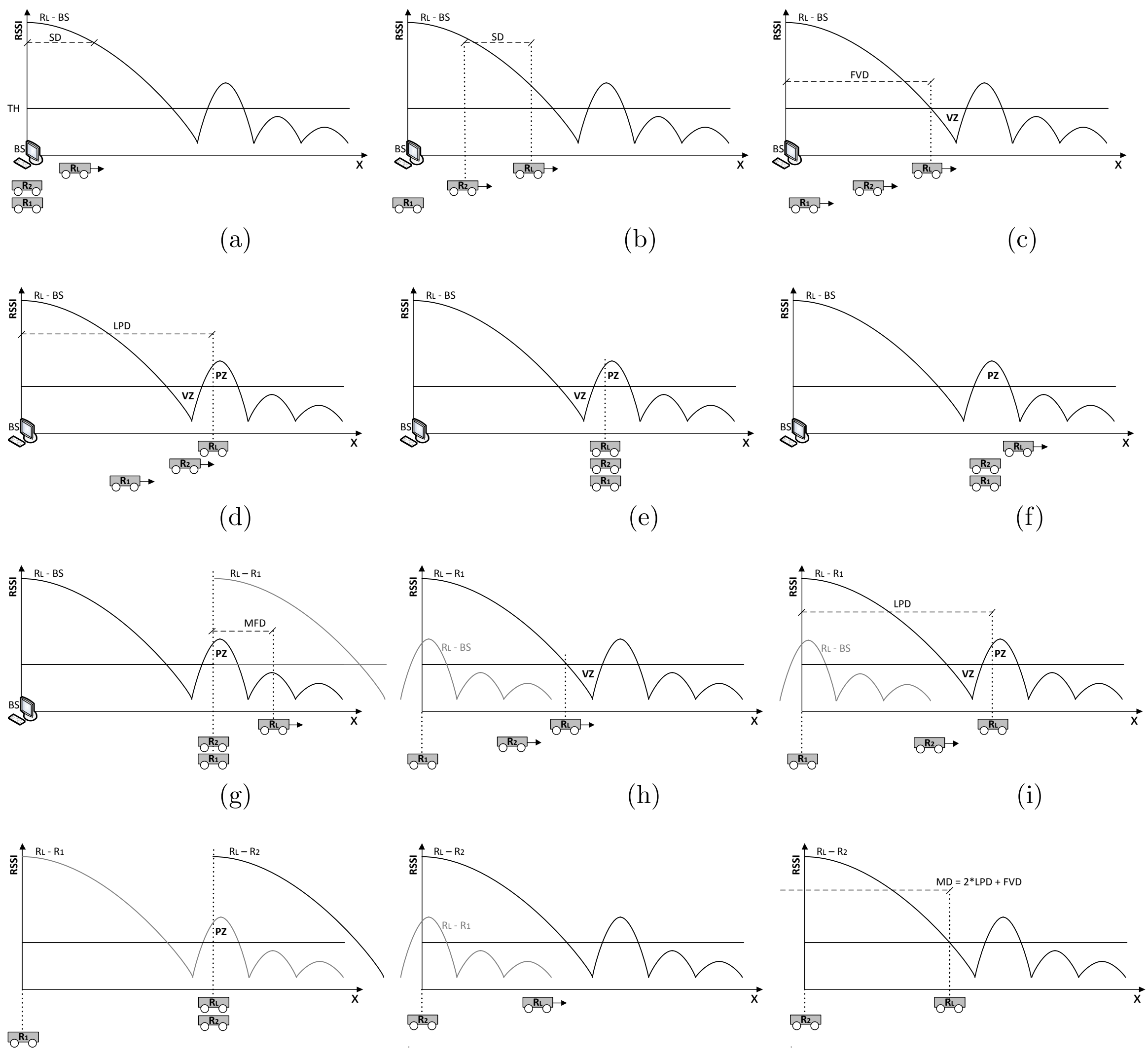
Table 6.5: Parameters and terms used in the planning strategy. N is the number of follower robots

Deployment parameters. Tuning for the Somport tunnel.

The analysis of the Somport tunnel performed in the Section 5.3.3, allows to compute the parameters (Table 6.5) of the planning algorithm in order to execute it in a real scenario. The first parameter is the safe RSSI Threshold (TH), defined to be the RSSI value that ensure a secure communication between nodes, avoiding packet losses. This is selected to be -70 dBm in this case, for the reasons described in Section 6.3.2. The RSSI value between the base station and at least one of the robots must be above TH in order to maintain the network fully connected. To guarantee that this level is maintained between two adjacent robots, we introduce the second parameter: the Safe Distance (SD). This is the maximum distance that two adjacent robots can move away from each other in order to maintain the RSSI above the TH. As can be seen in Figure 5.4, in the first 750 m from a transmission node (the *near sector*), the path loss and fast-fadings dominate. The idea is to avoid that a fast-fading could led a robot into an unsafe zone. Thus, based on the study, we selected SD to be 350 meters, where even with fast fadings fluctuations, the RSSI value is maintained above -70 dBm. The valley-zone (VZ) and peak-zone (PZ) are defined as zones below and above TH, respectively. Once the robot is located in a valley-zone, the goal is to look for the next peak-zone. The Maximum Fading Distance (MFD) is a parameter that represents the maximum exploration distance within a VZ in which the leader robot can search for a peak-zone before setting a follower as a fixed repeater. Based on our study, this distance was chosen to be 500 meters, that's the distance between two consecutive *slow-fadings*. If a peak-zone is not found within this distance, it doesn't make sense to continue looking for a peak-zone with this link. The algorithm sets a follower robot as a repeater and new *base*, and starts processing the signal with the latter. At last, in order to switch between zones, the RSSI should be maintained below or above TH for a distance greater than the Fast Fading Width (FFW), to avoid a switch in the state machine due to fast-fadings. Hence, FFW was defined to be the 20 meters, that is the maximum width of 94% of the fast-fadings in the Somport tunnel.

Deployment algorithm

Let R_L be the leader robot and $R_1, ..., R_n$ the follower robots. Although the algorithm is general, we assume $n = 2$ in this section in order to make easier to explain the algorithm. The main steps are drawn in Figure 6.22. The deployment begins with all robots close the base station in a chain configuration ($R_1..R_nR_L$) and ready to start. First, a goal is set at the Maximum theoretical Distance (MD) computed for the number of the robots available, and it is assigned to the leader robot. It begins to move toward this goal while sensing the quality of its link with the BS (Figure 6.22.a). When it reaches the limit of the safe distance (SD) from the closest robot, it creates a virtual rope between itself and the first follower R_n. It provokes the latter to start moving and following the leader at SD distance (Figure 6.22.b). Both robots continue moving until, again, the distance between the first and the second follower rises above SD. In this moment the second follower R_{n-1} starts moving to follow R_n. The process repeats with the other robots of the team until a chain of equidistant robots is created. The situation changes when the leader traveled a distance equal to the First Valley Distance (FVD) and enters a non-safe zone (valley-zone, VZ) in which its link-quality with the BS falls below the TH (see Figure 6.22.c). In this moment the communication between the leader and the BS is not yet direct, but R_L uses the nodes of the chain as relays to communicate with it. Even so, the leader continues moving toward its goal looking now for a new safe zone (peak-zone, PZ) to reestablish the link with the BS (see Figure 6.22.d). In this, it prepares to stop moving to verify that the peak just found is actually a PZ (and is not due to a fast-fading). This filtering is made discarding less than twenty meters wide peak-zones, the FFW parameter defined in Table 6.5. In the peak-zone, the leader stops and groups all the follower robots. During the grouping, the connectivity is guaranteed by the fact that the leader has a good link quality with the base and the distance among the robots is always below the SD. When the grouping is completed (see Figure 6.22.e), the algorithm restarts (Figure 6.22.f). The leader searches for the next peak. If the leader does not find a new peak-zone within the MFD (see Figure 6.22.g), it does not exist. When this situation takes place, the farthest follower (R_1) is fixed as



(a) (b) (c) (d) (e) (f) (g) (h) (i) (j) (k) (l)

Figure 6.22: Representation of the main steps of the planning algorithm. In a), Robots R_L, R_1 and R_2 from the pole position where base station BS, move along the tunnel, keeping the safe distance between them (b). When the leader R_L enters a non-safe zone (VZ), it uses the nodes of the chain as relays to communicate with the base station and continues moving toward its goal (c). R_L is looking for a peak-zone (PZ) to reestablish the link with the base station and calls all the following robots in that zone (d). When the grouping is completed (e), the algorithm restarts (f) and the leader moves forward. When the distance between the leader and the followers rise up to the MFD distance, a new base station is established for the leader in R_1 (g). R_2 follows R_L (h) when the distance between them rise up the safety distance and the leader continues moving until it find a valley but now with respect to the new base R_1 and to find a new peak (i) where to group again with R_2 (j). R_2 becomes a stationary relay as well (k) and the leader R_L reaches the limit of last safety zone (l), completing the chain that maximizes tunnel coverage with the available robots.

new base (it will not move anymore) and the leader starts to sense the link quality with respect to this new base (Figure 6.22.h). The leader continues moving until it finds a valley, but with respect to the new base R_1. Then it explores to find a new peak where the $n-1$ remaining followers are grouped (see Figure 6.22.i). After grouping (Figure 6.22.j), the process restarts. From this moment until the leader reaches the end goal all the follower robots are fixed as a new base, following the rules just described. Figure 6.22.k represents situations in which R_2 is the new base. The maximum distance is reached when the leader finds a valley-zone and the last follower robot has been already fixed as new base (see Figure 6.22.l).

The proposed algorithm uses the communication parameters TH, SD, FFW and MFD (see Table 6.5). These parameters are obtained from the analysis of the measurements described in the Chapeter 5 and the Section 6.3.2. A poor estimation of these parameters may affect the performance and proper functioning of the algorithm. A qualitative analysis of possible affections follows. The safe RSSI Threshold (TH) does not depend on the propagation characteristics of the tunnel but only on the communication system (hardware, modulation scheme, frequency, etc.). The Safe Distance (SD) is the most critical parameter. Its overestimation can cause loss of communication and, thus, mission failure. An underestimation would mean a decrease in deployment distance. The Maximum Fading Distance (MFD) is used as stop condition. A poor estimation does not represent a threat for the mission, but may increase the deploying time or decrease the maximum distance achieved. Finally, the Fast-Fading With (FFW) is only a filter parameter. An overestimation may decrease the exploration distance because a short peak zone can be interpreted as fast-fading, whilst an underestimation can cause an increase in the exploration time since fast-fading can be interpreted as peak-zones. The reactivity of the algorithm makes it insensitive to parameter variation in terms of safety. The algorithm can also enable an online signal analysis and then an auto-tuning process could be implemented.

Calculation of the Theoretical Maximum Distance

The calculation of the theoretical Maximum Distance (MD) is straightforward. Let LPD the distance from the Base Station to the last peak-zone in which the signal strength is above the threshold TH, and FVD the distance from the Base Station to the start of the first valley-zone (see Figure 6.22). This distance is reached when the leader traverses all the valley-zones up to the last peak with respect to each base, except the last established base, in which the leader stops before traversing the first valley. An upper bound of exploration distance is :

$$MD = n * LPD + FVD \tag{6.8}$$

being n the total number of followers. Achieving this bound depends on the relation between the SD, the width of valley-zones and the number of followers. The MD

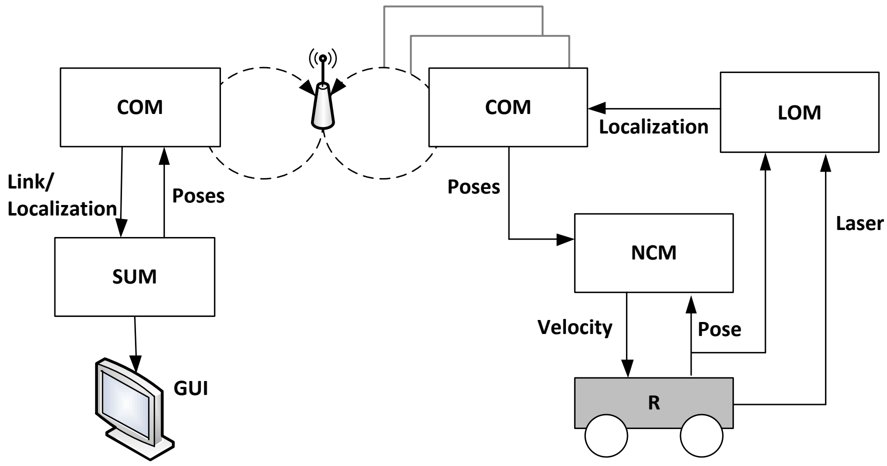


Figure 6.23: Software architecture for the base station and robots.

is used for planning the last goal to be stated for the leader robot. This goal is only a potential goal to be reached because, as explained at the beginning of this section, the plan for all the robots is computed in real time during the exploration, based on the real signal measurements. Moreover, is an estimation about how far the tunnel can be explored, and also a rough estimated value to compute the number of robots that are needed for the whole scenario. The general Algorithm 1 has been implemented by means of a state-machine. Several states are defined: $BEGIN$ when the algorithm starts, $FIND\_VALLEY$ when the leader is finding the first valley under TH, $FIND\_PEAK$ when the leader is finding a peak zone, $GROUP\_ROBOTS$ when all the robots move for grouping in a location, END when the exploring maximum distance is achieved. The parameters defined in Table 6.5 are used in different states of the algorithm.

6.3.3 System Description

In order to implement the multi-robot system for the application addressed in this work, we developed a distributed architecture that integrates different modules in each robot: a COMmunication module (COM), a Navigation Control Module (NCM), a feature-based robot LOcalization Module (LOM) and a SUpervisor Module (SUM). This software architecture was implemented on the onboard computers which run the modular solution presented in Figure 6.23 and replicated in each robot:

- The COM module provides multi-hop, real-time communication among robots and base station. It is in charge of routing the signal quality, the navigation information and robot localizations over safe paths.

Algorithm 1

```
base = 0, state = BEGIN
while true do
    if state = BEGIN then
        R_L ← goal(MD)
        for i in followers do
            set_rope(R_i, R_{i+1}, SD)
        state ← FIND_VALLEY
    else if state = FIND_VALLEY then
        if found_valley(R_L, R_base, TH, FFW) then
            if Card(followers) > 0 then
                locValley ← locR_L
                state ← FIND_PEAK
            else
                stop(R_L)
                state ← END
    else if state = FIND_PEAK then
        if dist(locR_L, locValley) ≥ MFD or
                        dist(locR_L, locValley) ≥ Card(followers) * SD then
            set_new_base_station(R_{base+1})
            state ← BEGIN
        if found_peak(R_L, R_base, TH, FFW) then
            stop(R_L)
            for i in followers do
                R_i ← goal(R_L)
            state ← GROUP_ROBOTS
    else if state = GROUP_ROBOTS then
        if robots_grouped then
            state = BEGIN
    else if state = END then
        exit
```

- The NCM module implements the motion planning and reactive navigation techniques and generates velocity commands for the robots, providing a safe navigation towards the goals assigned by SUM (see below). It uses the information of the robots' sensors (odometry and laser rangefinder) combined with the localization provided by the LOM module, in order to achieve the navigation.

- The LOM module provides a global localization of the robots, using the information of the rangefinder and odometry sensors and a pre-existent map. This localization information is sent to the COM module that, in turn, sends it through the network to the base station.

- The SUM module is in charge of collecting the flow of system information (links state, robot localization, etc.) from the network and sending commands to the other modules (goals, emergency stops, resumes, etc.). The base-station generates such commands, once requested by the operator through its GUI.

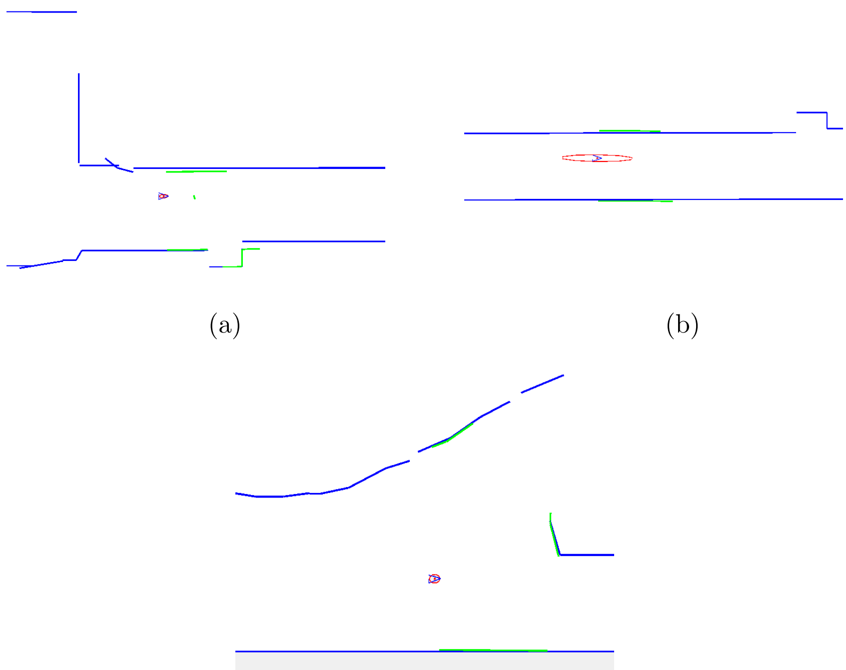
All the system has been implemented in the ROS [Quigley 09] platform. Each node uses its own core and all the communication among different nodes have been carried out using the *ros_rt_wmp* node [Tardioli 12a] that allows the real-time multi-hop communication among the different ROS nodes distributed in different cores.

6.3.4 Communication Module

The communication among the robots and between them and the base station must obey to a set of important conditions and characteristics. Above all, since our solution needs information about the link quality amongst robots and share some navigation information, as the localization and several time sensitive data, the COM module must be capable of capturing the link state about each pair of robots and transport information in a network with real-time guarantees. This last requirement also involves the need of message priority in order to support multiple flows of data. Moreover, the network protocol must support multi-hop communication that is needed by the planning algorithm presented in Section 6.3.2.

The RT-WMP protocol: In order to fulfill the role of providing information transport with the previously cited characteristics, the COM module bases the communication in the RT-WMP protocol, widely described in the Chapeter **??**.

The Link quality Matrix: In environments that offers serious signal fadings, if nodes are moving, the radio signal, and therefore link quality amongst them, could change rapidly and it must be reflected in the global status of the network. Consequently, when a node discovers a change, it has to propagate this information



(a) (b) (c)

Figure 6.24: Mapping and robot localization. Three typical zones found in the tunnel. Vaults (a) and galleries (c) allows accurately localize the robots, long corridors (b) favors the uncertainty increase (red ellipse). In blue the previous map, in green the features matched with the map.

as soon as possible. In RT-WMP this task is automatically carried out by the protocol token, so global network link state is updated in each protocol round.

How we have seen in the Section 2.4, the protocol defines the so called Link Quality Matrix (LQM). Each column of the matrix describes the link quality of any node with its neighbors in terms of the RSSI. From the point of view of communication transport layer, COM module uses LQM to find a reliable path over which to send user or managements messages.

6.3.5 Localization Module

For a robust autonomous navigation it is necessary to continuously localize the robots as precisely as possible. The technique used is based on the one described in [Lazaro 10]. A segment-based map is built using a laser rangefinder, which will be used as an a priori map for the real time localization while navigating. The LOcalization Module (LOM) provides the robot pose during the exploration. The Extended Kalman Filter localization algorithm segments the laser sensor readings and matches the features obtained with the set of those representing the map. The laser sensor segmentation technique is based on a tracking-like algorithm combined with a validation gate used to group the range readings into regions. These regions are successively split into segments, which describes the environment seen by the robot through a polygonal approximation technique. Figure 6.24 shows some snapshots of the localization algorithm output. It shows the position of the robot during an experiment, the map (blue lines) and the correctly matched observations (green lines). It is worth noting that in this kind of environments like straight tunnels the uncertainty in the motion direction (x axis) continuously increases, because of the planar walls. However, in the particular tunnel of the experiments, the vaults and the lateral galleries allows to periodically strongly reduce this uncertainty. This can be observed in Figure 6.24.a,c, in which the ellipse representing the uncertainty has been reduced, against the drew in the Figure 6.24.b.

6.3.6 Navigation Module

The goals to be reached by each robot in every moment are set by the planner, as explained in Section 6.3.2. The navigation control module (NCM) is in charge of providing a safe navigation to a given goal. In order to navigate autonomously in such environments, each of the robots incorporates a navigation system based on the Obstacle-Restriction Method (ORM) [Minguez 05]. This algorithm is an obstacle avoidance method that obtains similar results to the Nearness Diagram family methods [Minguez 04], [Minguez 01] in dense and complex scenarios, but improves trajectory behavior in open spaces. Furthermore, to overcome the limitation of the speed when no obstacles nearby, the ORM algorithm have been improved in a similar way described in the Section 6.2.6.

6.3.7 Supervisor Module

The Supervisor Module is in charge of executing the deployment algorithm (presented in Section 6.3.2) and controls the whole system. It executes the state machine using the information provided by all the nodes involved in the system through the COM module like:

- *Locations of mobile robots*: the robots send periodically its locations to the SUM module using a real time flow provided by the COM module.
- *Signal Strength among nodes*: the LQM shared among nodes is provided by the COM module to make the SUM aware about the connection of the network and the link quality among them.

The SUM module also uses the COM to send *goals* or *stop* commands to the mobile nodes in order to ensure the correct execution of the algorithm. Other informations, as laser scans, can travel through the communication network for monitoring purposes. These information flows have a lower priority to avoid the risk of delaying the information needed for control. The SUM also has a graphics

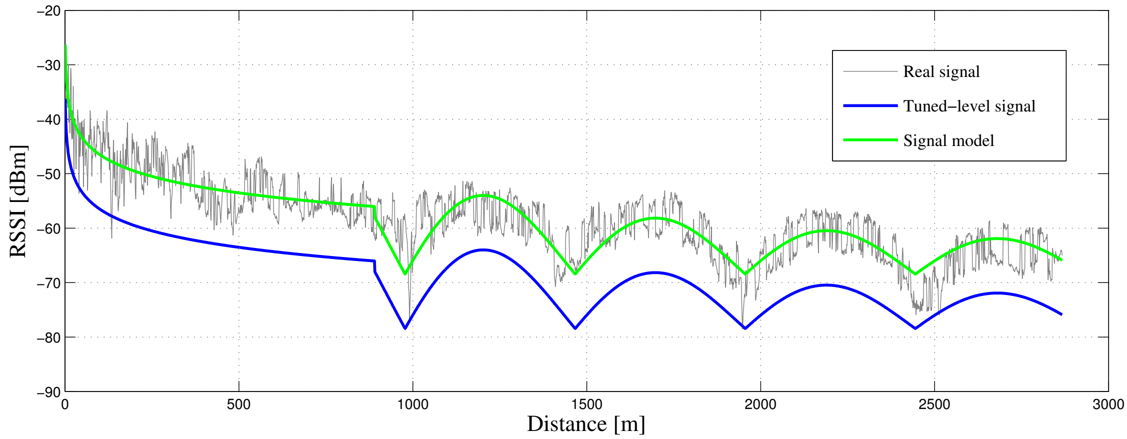


Figure 6.25: Real signal and signal from the model.

user interface (GUI) that permits the visualization of the system state, the link quality among the nodes and the laser readings of each robot.

6.3.8 Experiments

The evaluation of the system has been carried out both by means of simulations and field experiments. The simulations have been performed using a simulated signal to verify the correctness of the algorithm. The field experiments have been performed in the Somport Tunnel already described in Section 6.24c. In all the experiments the parameters shown in Table 6.5 have been used.

Propagation function model

As we showed in Section 5.3.3, the propagation of the signal in the tunnel exhibits a characteristic shape that we modelled by the *Sinc* Function 5.1.

The level of the signal used for simulations has been lowered for bounding the duration of simulation and to simplifying the execution of the algorithm maintaining the same TH level. In this way, only two peak-zones will appear during the simulation. In Figure 6.25 the measured signal and the computed ones are shown.

A simple analysis of the function allows to automatically compute how many slow-fadings and the local maxima there are in which the signal is above the established threshold TH by solving:

$$\nabla_x y(x) = k \cdot \frac{\frac{\pi}{(\lambda} \cdot cos(\beta) \cdot x - sin(\beta))}{x^2} = 0 \tag{6.9}$$

being $\beta = \frac{\pi}{\lambda} \cdot x$, which yields to the equation,

$$M = solve(tan(\beta) = \beta) \tag{6.10}$$

being $M = \{m_1, ..., m_{n_f}\}$ the location of the local maxima found above the threshold corresponding to the n_f slow-fadings.

From this value the estimation of the maximum distance LPD defined in equation 6.8 and the last maximum used to set the initial goal for the leader robot can be computed.

Simulation Results

The complete system has been simulated using the previously calculated signal shown in Figure 6.25. Three mobile robots has been used for simulation within the Stage simulator within the ROS environment and executing the same code as for the real experiment. The three robots started in a chain configuration close to the base station. The results are presented in Figure 6.26.a and 6.26.b. The Figure 6.26.a shows the movement of the robots along the tunnel. The distance of the leader robot R_L with respect to all the other nodes begins to rise when it starts moving (a). After 350 meters, in point (b), the distance between R_L and R_2 rise above the SD and the latter starts to move. After that, the same happens between R_2 and R_1 and the latter starts to move (c). At the same time the leader finds a valley-zone with respect to the base station (BS) in (d). The leader continues moving up to the moment in which it reaches a peak zone (e) and stops. It calls its followers that reach the leader in (f). The algorithm restarts and a similar situation takes place in points (g), (h), (i) and (j) where the leader collects the followers again. After that the leader restarts and after finding a VZ in (k) continues looking for the next PZ pulling R_2 in (l). When it reaches point (m), R_L has explored the valley-zone covering a MFD distance and then R_1 is fixed as new *Base*. From this point on, the leader starts to sense its link with R_1. When it realizes that is in a peak zone with respect to R_1 (n) it calls R_2 that reaches the leader in (o). After that, the algorithm restarts again with only one follower. The leader traverses the valley-zones (p) and (q) with the help of R_2 reaching the peak zone in (v) where it calls again R_2 which stops in (w). The leader restarts, and find a new valley-zone in (x). In (y) it tries to pull R_2 again but it has to stop in (z) to avoid leaving the peak zone where it is and that permits the communication with R_1. The leader fix it as new base and continues exploring until the link that connect it with R_2 is above TH. According to equation 1, the estimated Maximum Distance (MD) is 4.400m (LPD=1750, FVD=900), which fits with the final position reached by the leader in the simulation.

The Figure 6.26.b shows the (simulated) link qualities obtained during the execution of the experiments. As it is possible to see, the signal level of R_L with the *base* fixed at any moment or with the closest follower is always above TH. In the points (m) and (z) (corresponding to the ones in the Figure 6.26.a) it is possible to observe a sudden change in terms of RSSI due to the base switching. As described, in fact, in (m) and (z) R_1 and R_2 become the new base respectively. It is also possible to observe that, as expected, the signal is repeated with the same

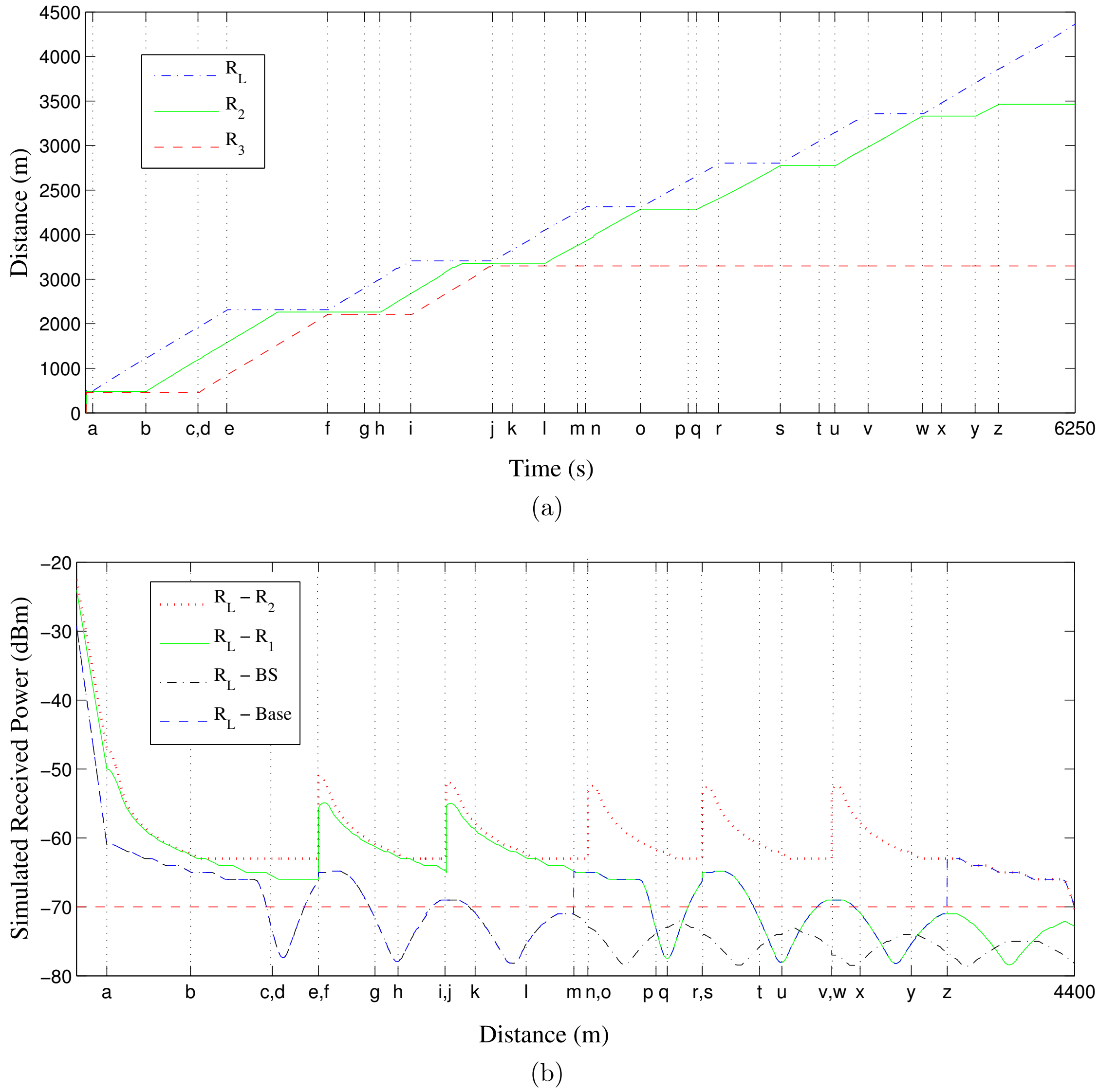


Figure 6.26: a) Robots' position versus time, b) Signal quality versus position. R_L starts (a). R_L finds a peak zone $(e, i, n, r$ and $v)$. R_L finds a valley-zone $(c, g, k, p, t$ and $x)$. Robots meeting points $(f, j, o, s$ and $w)$. Base switching $(m$ and $z)$. Leader pulls followers $(b, d, h, l, q, u$ and $y)$.


Figure 6.27: Two snapshots from the real experiment.

shape after each meeting of the robots ((f), (j), (o), (s), and (w)) and after every switch (m) and (z).

Field experiment

After completing the simulation experiments, we carried out a field experiment in the Somport Tunnel (described in Section 5.3). Figure 6.27 shows some instances in the experiment. The objective was to verify the results in a real-world scenario using mobile robots and actual wireless communications. We used three Pioneer P3AT mobile robots controlled by three Dell D630 laptops. At the base station we used a Getac B3000 Rugged laptop. All the wireless devices were Ubiquiti Networks SRC 802.11 a/b/g PCMCIA cards based on the Atheros 5004 chipset. For all the nodes we used a dual band 5.2/2.4 GHz Omnidirectional Antenna with a gain of 4.5 dbi in the 2.4 GHz band. The transmission power was fixed at 10 dBm and the frequency at 2.412 Ghz (channel 1 on *802.11 g* band) while the data rate was fixed at 6 Mbps.

The results are shown in Figures 6.28.a and 6.28.b. Additional videos are available at [Multimedia 12]. Only the stretch between 1750 meters and 3000 meters has been selected to be shown for being the most interesting and with the end of the making the figure easily understandable. Figure 6.28 shows the results of the experiment from the moment in which robot R_L starts to move after its stop at 1750 meters. At moment (a) it finds a valley-zone but continues moving up to the point at which the distance with respect to R_2 exceeds the SD (b). At this moment, R_2 starts to move to follow the leader but a few meters on, the latter finds a PZ in (c) where it stops and calls the followers. It is possible to appreciate a slightly different speed between the two robots due to R_1 having different mechanical parts with respect to the other robots.

When both followers reach the leader at (d), the latter restarts its movement and at (e) finds another VZ. It continues moving up to the moment in which the distance between itself and R_2 again exceeds SD (f) at which point the latter starts following R_L. After that, in (g) the MFD is reached and R_1 is fixed as the

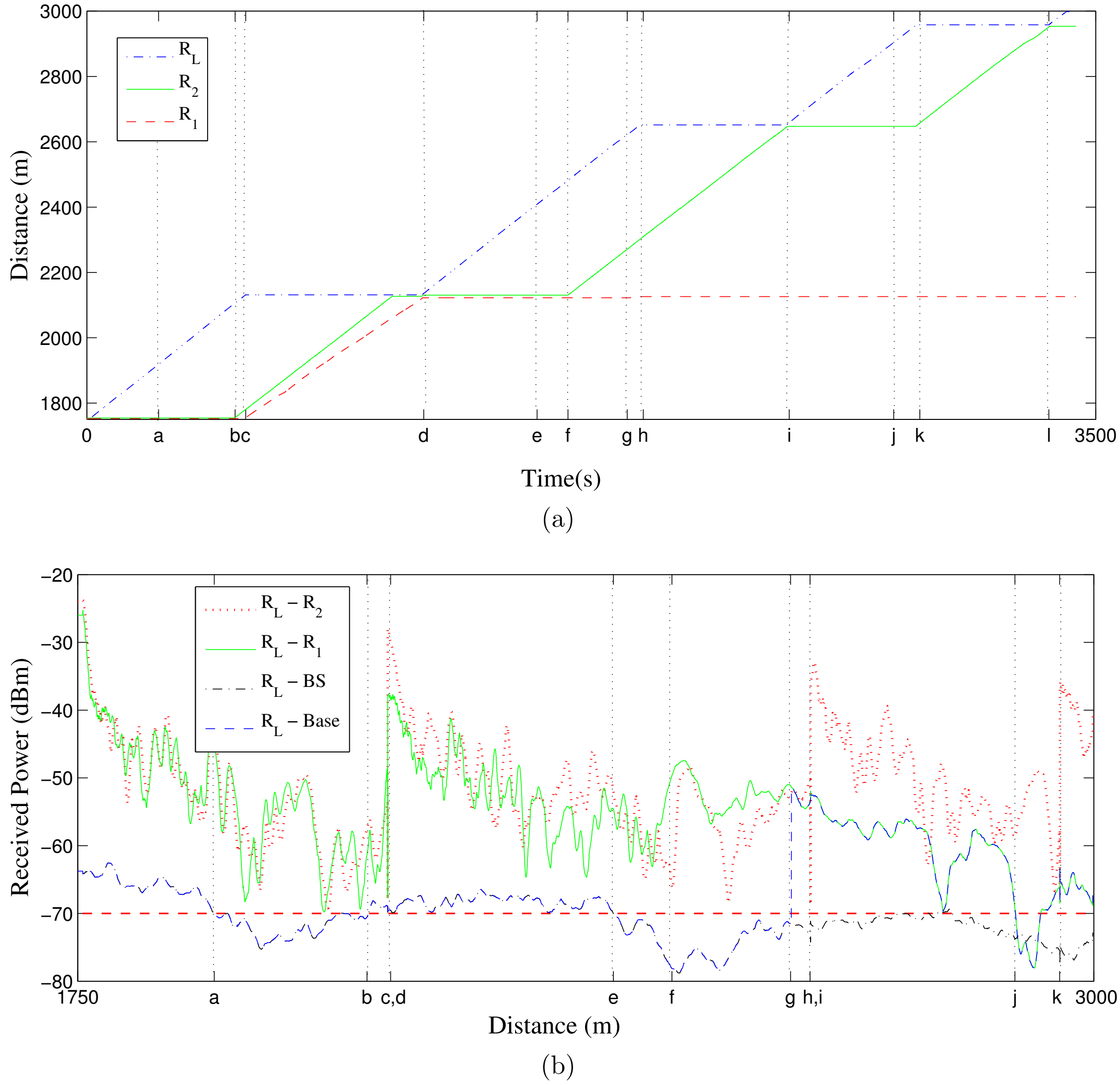


Figure 6.28: a) Robots positions versus time. b) Signal versus position. R_L found a valley-zone (a, e and j). R_L finds a peak zone (c, h and k). Meeting points (d, i and l). Leader pulls followers (b and f). Base switching (g).

Path	Count	Percentage
$BS \rightarrow R_1 \rightarrow R_2 \rightarrow R_L$	12183	35.8%
$BS \rightarrow R_2 \rightarrow R_L$	11649	34.3%
$BS \rightarrow R_1 \rightarrow R_L$	1543	4.5%
$BS \rightarrow R_L$	8659	25.4%

Table 6.6: Path of the messages from leader to base station.

new *base*. From now on, the leader starts sensing the link quality with respect to this new *base*. In the new PZ, the leader stops and waits for R_2 which reaches R_L at (h). At this point the latter restarts and, after passing a valley-zone (j), finds another peak in (k). Again it calls its only follower (l) and the process restarts.

Figure 6.28.b shows the signals. It is possible to see the beginning of the VZ (a), (e) and (j) and the PZ (c), (h) and (k) and the switching between the base BS and R_1 in (g). It is also possible to observe that the signal between the R_L and the fixed base or between R_L and its closest follower is above the TH limit at any moment. Also, it is interesting to appreciate the repeatability of the signal after each grouping of the robots.

As expected, during the whole duration of the experiment, the communication was permanently maintained among all the nodes of the network. The varying position of the nodes have provoked different network topologies throughout the experiment and the need for multi-hop communications, as confirmed by Table 6.6 which shows the paths that have been used by the messages sent from the leader node (odometry, position, etc.) to reach the base station and their respective percentages. The specific distribution of these percentages depends in part on the routing algorithm that, in the case of RT-WMP, favors longer safer paths over shorter dangerous ones. Figure 6.29 shows the RSSI of the weakest link of the chosen path at any moment. Analyzing Figures 6.28.b and 6.29 together, it can easily be inferred that the communication would not be possible without multi-hop support. In fact, the first figure shows that in many cases the RSSI of a single link falls below the minimum admissible threshold TH but the second confirms that all the paths used during the operation of the system accomplish the goal of having all the links above such a safety level. This fact has permitted the PDR to be above 99.5% during the whole duration of the experiment, as expected given the results described in Section 6.3.2.

6.3.9 Conclusions

A technique for planning the development of a team of robots in confined and fading environments has been addressed. It has been integrated in a complete system through a distributed architecture, in order to work in real environments. Two were the main objectives: i) to maintain in every moment the network connectivity; ii) to reach the maximum distance in the exploration with the available robots. To

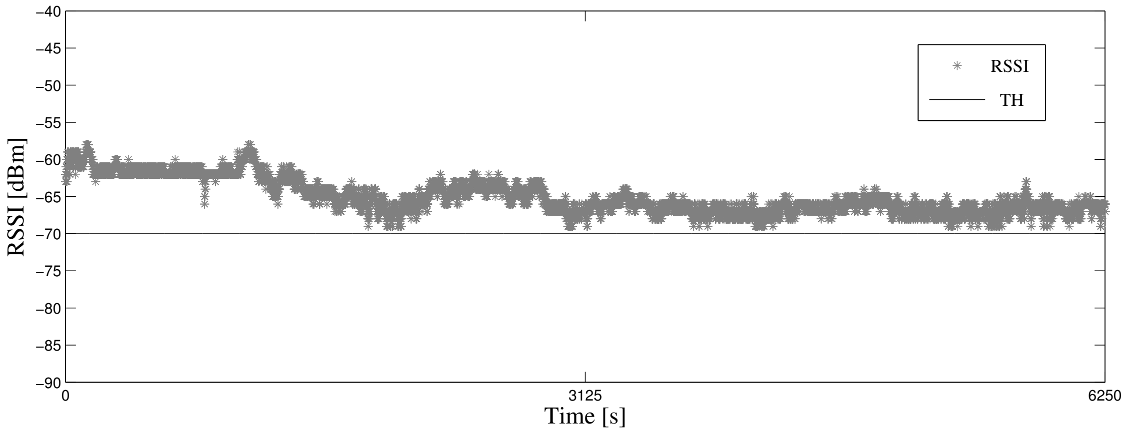


Figure 6.29: Received Signal Strength of the weakest link in the message path.

simultaneously achieve both objectives, the communications among all the elements of the network, robots and base station, have to ensure that the signal strength maintains above a threshold which allows to transmit and receive at maximum PDR. Taking into account the signal analysis carried out in these specific scenarios, the technique uses the signal parameters to particularize the planning. So, it will be necessary to estimate those parameters for other fading-like scenarios, but the strategy is general. The leader robot uses the real signal measured by it to plan its motion in real time and the deployment of the follower robots which act as repeaters.

As main conclusions and lesson learned from the exhaustive experiments achieved in the tunnel, we highlight the following. The signal in this kind of environments has a typical shape, in which slow-fading a fast-fading appear. This shape allows to enlarge the multi-robot deployment in such a way we can maximize the distance to be reached with the available robots without lost of connectivity in the network. The slow-fadings are fundamental in the planning strategy, because it profits them to place the robots for maintain the maximum PDR. The simulated and real experiments along three kilometers of the tunnel back the good performance of the planning technique based on the signal strength parameters. In both scenarios, the simulated and the real one, the plan worked as foreseen, even although the simulated and real signals had not exactly the same behavior. The message routing technique always maintained in the real experiments, by choosing in every moment the most suitable robot in the multi-hop network.

Several aspects remain open yet. The problem of minimize the number the robots to reach a desired distance, can be seen as a complementary problem to be solved. More experiments would be necessary in other tunnels or galleries to finish a more general characterization of the signal propagation. Other issues than can be studied are the antenna diversity to minimize the impact of transversal fadings and the navigation using quality signal maps of confined environments.

Chapter 7

Conclusions

7.1 English

This PhD thesis has focused on the RT-WMP, one of the few implemented real-time wireless protocols for MANETs, developed at the University of Zaragoza.

The work includes an in-depth evaluation and analysis of the protocol, a proposal for a QoS extension, a study about its use in confined environments and the demonstration of the effectiveness of the protocol in field applications. The work has been developed within the framework of the NERO, TESSEO and SICRA Spanish National Projects and the URUS European Project.

This work complements other research present in the literature, which in recent years has been aimed at offering new wireless communication solutions taking into account the challenges posed by the need to maintain multi hop routes despite the problems of mobility, signal interference, multiple access channels, fading effects, limited bandwidth and power constraints. These aspects have a noticeable impact on applications that require real-time capabilities, where the correctness of task execution is normally expressed as a set of timing constraints that the system has to meet at run-time.

The first contribution of this thesis is an in-depth analysis of the performance of the protocol in order to determine its effectiveness and examine the possibility of verifying a priori that the protocol timing requirements can be met in all circumstances. This work was developed through a theoretical characterization, a set of real tests and a complete analysis of the protocol. Firstly, we have shown how each RT-WMP event/phase has a bounded and known duration and how the protocol offers a similar bandwidth to that offered by the 802.11 plain protocol both in worst-case multi-hop situations and in relatively small and completely connected networks. Secondly, extensive real tests, carried out using specific hardware, have demonstrated that the protocol is capable of offering a good worst-case real-time communication bandwidth for different networks sizes, respecting priority delivery and fairness and with bounded worst-case end-to-end delay. The results are interesting because they take into account the worst-case situation and, moreover, they do not require additional overhead due to a routing protocol that must be used on top of the plain 802.11. Furthermore, unlike many of the measurements presented in the literature which in the majority of cases are only simulated, we have made a comparison with the well-known general purpose protocol OLSR both in terms of worst situation bandwidth and mobility capabilities. This actual comparison has shown how general purpose routing protocols can not easily be used for time-sensitive mobile applications due to the unpredictability of the end-to-end delay, to the absence of priority support and to the poor performance in terms of mobility management. Finally, an in-depth analysis has been carried out in order to verify the possibility of using such a protocol as a communication framework in distributed real-time systems. The analyzability has been considered through the capability of planning of tasks and resources, the estimation of overhead, the blocking and a controlled overload. These results are contained in the article "A Wireless Multi-hop Protocol for Real-Time Applications" that was submitted for publication in the Ad Hoc Networks international journal.

The protocol has been successively extended to take into account the need for multimedia flow support, for example in rescue operations where humans may be involved. To manage this kind of flow simultaneously with the real-time flow, we have proposed a mechanism to add Quality of Service capabilities that offer the possibility of establishing voice and video links without altering the worst-case characteristics of the protocol. TThe QoS extension takes advantage of the bandwidth left free by the protocol when it is not working in the worst-case situation, using it to send audio and video streaming flows. It also includes a technique to control the access to the network of new flows. This novel contribution has been implemented and evaluated. The results were presented at the First International Conference on Ad-Hoc Networks in Niagara Falls, Canada and published in the "Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering" under the title "QoS over Real-Time Wireless Multi-hop Protocol".

The great interest in rescue applications in disaster scenarios involving humans in confined environments such as tunnels or mines has led us to consider the problem of providing an efficient communication service in these areas. This stems from the fact that common radio systems can provide at best very limited communications capability in such environments. In this context, the novel and empirical contribution of this thesis has been a study of the possibility of applying the protocol in underground areas and performing a set of real measurements. The relation amongst link metrics, coverage range and the effect of the environment on the signal propagation have been taken into account in the characterization of so-called fading environments with a view to providing real underground communication applications using MANETs.

In fact, the last contribution of this thesis is the carrying out of a set of three field experiments in underground settings where the protocol performance and effectiveness are shown from the points of view of real-time characteristics, QoS capabilities and specialization to the specific environment.

The first application is the use of the RT-WMP jointly with the QoS extension used in this case to manage multimedia communication between a pair of mobile nodes in a confined environment represented by a linear tunnel, the Somport tunnel linking Spain with France. In the experiment, a set of nodes were deployed along the tunnel and placed at strategic points to act as backbone relay nodes for two freely moving mobile stations. A previous analysis of the propagation in the tunnel enabled the backbone nodes to be positioned so as to minimize the multipath effect. The specific topology and situation led to a specialization of the RT-WMP protocol to better perform routing messages in this type of environment, taking advantage of the a priori knowledge of the topology and supporting the mobility of the end nodes.

The whole system was finally tested in the Somport tunnel in the presence of the tunnel crew, the director of the road unit of the province of Huesca and representatives of the Spanish Ministry of Public Works with satisfactory results on 23 August 2009 and again on 19 July 2010. A voice link was established between the two mobile nodes, one of which was moving along a stretch of about 7.5 km at a considerable speed. The voice was clear and with no interruptions, demonstrating the validity of the improved routing algorithm, the effectiveness of the variable-priority delivery algorithm and the validity of the previous study that resulted in the backbone nodes deployment. Part of this work presented at the third International Conference on Wireless Communications in Underground and Confined Areas, while the complete results were published in the Ad Hoc Networks international journal under the title “Real-time wireless multi-hop protocol in Underground Voice Communication”.

The second experimental application presented in this thesis involved real robots and human operators in a whole system, performing a real exploration in the Somport tunnel.

Several robotics issues such as motion control, cooperative navigation and perception, localization and, of course, communication were involved, taking into account the specific environmental characteristics. The task was exploring the tunnel by a team of two robots controlled by a base station. The challenge was to perform the whole semi-autonomous exploration without losing the connectivity of the network at any moment. The goal of reaching a shelter located at a considerable distance and, above all, in the absence of line of sight between the base station and the lead robot while maintaining vocal and visual communication was completely achieved. This was possible by implementing a communication module integrated into the whole system capable of managing the real-time traffic used for the cooperative robot control and the QoS flows for the multimedia traffic. The results of this work were presented at the ROBOT2011 Workshop held in Sevilla in November 2011under the title “Robot teams for exploration in underground environments”.

The last application presented in this thesis is a novel planning technique to deploy a team of several robots along a tunnel capable of maintaining network connectivity at all times and to reach the maximum possible distance in the exploration with the robots available. In this context, connectivity capabilities in underground environments play an essential role. The idea was to take into account the signal analysis carried out in these specific scenarios. The technique uses the signal parameters to particularize the planning. Thus, the leader robot uses the real signal it measures to plan its motion in real time and the deployment of the follower robots which act as repeaters with the base station.

This work involves several contributions. Firstly, a technique was developed to drive the deployment using the parameters obtained by the signal propagation analysis. Secondly, a general strategy for this kind of environment in which the signals exhibit similar behavior was implemented. Finally, the complete system was evaluated by means of simulation and in a real scenario along three kilometers of the Somport tunnel with satisfactory results. The satisfactory results of this contribution will be published in the special issue on Robotic Communications and Collaboration in Complex Environments of the International Journal of Robotics Reserch (IJRR) under the title “Signal Based Deployment Planning for Robot Teams in Tunnel-like Fading Environments”.

In summary, we have presented a complete study of a real-time wireless framework offering the possibility of simultaneously managing QoS flows. The system was developed, extensively tested and improved in efficiency by adapting its functionalities to the features of the hostile environment in which it was designed to operate. The effectiveness of the proposed solution was demonstrated in real applications in underground environments, involving mesh networks and robot rescue teams.

Future work

Improvements and additional effort are required on several fronts. On the protocol side, one of the main challenge is to decrease the overhead introduced for the phases of the protocol that increase using the QoS extension. This overhead has an influence on the protocol scalability, which is limited.

A second challenge is to complete the integration of the QoS mechanism in a cross-layer architecture to improve its efficiency. This is possible by adapting the QoS load coming from the application layer or the available network resources estimated in run-time. Another interesting improvement of the QoS mechanism would be adding a multicast technique to allow communication amongst users in conference style.

From the point of view of performance analysis, a limitation is the comparison with the protocols found in the literature. The vast majority of these are proposed and tested only in simulation environments. The implementation of our solution in one such emulator may be useful to demonstrate its validity with respect to others.

From the point of view of environmental adaptation, more experiments are necessary to obtain a more general characterization of the signal propagation. For example, our work did not consider the impact of transversal fadings that could be limited using antenna diversity.

7.2 Español

Esta tesis se ha centrado en la RT-WMP, uno de las pocos protocolos implementados para las redes MANETs inalámbricas de tiempo real, desarrollado en la Universidad de Zaragoza. Las principales aportaciones de este trabajo han sido una detallada evaluación y análisis del protocolo, una propuesta de una extensión de QoS, un estudio sobre su aplicación en entornos confinados y la demostración de la eficacia del protocolo en aplicaciones de aplicaciones de robótica cooperativa y en redes malladas. La tesis ha sido desarrollado en el marco de los proyectos nacionales NERO, TESSEO y SICRA y del proyecto Europeo URUS.

El trabajo ha seguido la linea de investigación presente en la literatura, que en los últimos años ha tenido como objetivo ofrecer nuevos soluciones de comunicación inalámbricas con el fin de ofrecer un conjunto de características para hacer frente a la necesidad de mantener las rutas multisalto a pesar de la movilidad, a la interferencias de señal, al acceso múltiple al canal, a la propagación en entornos confinados, al ancho de banda limitado y a las limitaciones de potencia. Estos aspectos tienen un impacto notable en la aplicación que necesitan requisitos de tiempo real.

La primera contribución de esta tesis ha sido realizar un extenso análisis de las características del protocolo.

Este trabajo se ha realizado a través de una caracterización teórica, un conjunto de pruebas reales y un análisis completo del protocolo. En primer lugar, hemos mostrado cómo cada fase tiene un duración acotada conocida y cómo el protocolo ofrece un ancho de banda similar a al del protocolo 802.11, evaluado en una red multisalto completamente conexa, considerando el peor caso. En segundo lugar, las extensas pruebas reales, llevadas a cabo utilizando hardware específico, han demostrado que el protocolo es capaz de ofrecer una comunicación de tiempo real con satisfactorio ancho de banda para distintos tamaños de redes, respetando prioridad y retardo acotado en la entrega de los mensajes. Los resultados han sido interesantes, teniendo en cuenta la situación de pero caso y que no hay que considerar la sobrecarga debido a un protocolo de enrutamiento sí debe ser utilizado por encima del protocolo 802.11. Además, a diferencia de las mediciones presentes en la literatura, la mayoría de las cuales resultan simuladas, se ha realizado una comparación con el protocolo de proposito general OLSR, tanto en términos de ancho de banda como en movilidad. Esta comparación, efectuada con tráfico real, ha puesto de manifiesto cómo los protocolos de enrutamiento de propósito general no pueden utilizarse en aplicaciones de tiempo real debido a la imprevisibilidad del retardo extremo a extremo, a la ausencia de soporte de prioridad y a una limitada gestión de la movilidad.

Por último, se ha propuesto una definición del protocolo dentro de un análisis holístico al fin de verificar la posibilidad de utilizar un protocolo de comunicación en sistemas distribuidos de tiempo real. El analizabilidad se ha considerado a través de la capacidad de planificación de las tareas y los recursos, la estimación de la sobrecarga, del bloqueo y del control de carga del procesador.

Estos resultados se han reflejado en el artículo “A Wireless Multi-hop Protocol for Real-Time Applications” que fue enviado para ser publicado en la revista Ad Hoc Networks.

El protocolo ha sido ampliado sucesivamente para tener en cuenta la necesidad de dar soporte al tráfico audio/video que puede ser util, por ejemplo, en operaciones de rescate donde los seres humanos pueden estar involucrados. Para poder manejar este tipo de flujos simultáneamente con el tráfico de tiempo real, se ha propuesto un mecanismo con capacidades de Calidad de Servicio que permite establecer enlaces de voz y video sin alterar las características de peor caso del RT-WMP. Debido a que el protocolo basico trabaja solo esporadicamente en la situación de peor caso, la extensión de QoS se basa en utilizar el ancho de banda que queda libre cuando el protocolo no se encuentra en esta situación y utilizandolo para enviar mensajes audio y vídeo. Además, incluye una técnica para controlar el acceso a la red de nuevos flujos. Esta nueva característica ha sido implementada y evaluada en sistemas reales. Los resultados han sido presentado en Niagara Falls, Canadá en “the First International Conference on Ad-Hoc Networks” y publicados en el “Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering” con el título “QoS over Real-Time Wireless Multi-hop Protocol”.

El creciente interés en las aplicaciones de rescate que involucran seres humanos en entornos confinados, como túneles o minas, nos ha llevado a considerar el problema de proporcionar un servicio de comunicación eficaz en estas entornos. Esto deriva del hecho de que los sistemas radio tradicionales que se utilizan in estos caso proporcionan una capacidad de comunicaciones muy limitada. En este sentido, la novedosa aportación de esta tesis doctoral se plantea como un estudio empírico por medio de la realización de un conjunto de mediciónes reales para aplicar el protocolo en redes MANETs en entornos subterráneos. En la caracterización del entorno se ha tenido en cuenta la relación entre parámetros de calidad de enlace, rango de cobertura y el efecto denominado de fading en la propagación de la señal en tuneles. Todo esto en vista de realizar aplicaciones reales de comunicación subterráneas que utilizan MANETs.

De hecho, la última aportación de esta tesis es la realización de tres aplicaciones de campo en entornos subterráneos, donde se demuestra la eficacia del protocolo desde el punto de vista de las características de tiempo real, de calidad de servicio y la especialización al entorno específico.

La primera aplicación presenta el uso del protocolo RT-WMP conjuntamente con la extensión de QoS que, en este caso, se utiliza para gestionar la comunicación multimedia entre dos nodos móviles en un entorno confinado representado por un túnel lineal de Somport, que une España con Francia. En el experimento, se desplegaron un conjunto de nodos a lo largo del túnel en puntos estratégicos para actuar como nodos de retransmisión para los nodos móviles. El análisis anteriores de la propagación en túnel permitió el posicionamiento de los nodos fijos con el fin de minimizar efecto de multi-path. La topología específica de esta aplicación condujo a una especialización del enrutamiento de los mensajes, aprovechando el conocimiento a priori sobre la topologia fija y de manera que fuese facilitado la movilidad de los nodos de comunicacion.

El sistema completo se probó finalmente en el túnel de Somport a la presencia de la personal del túnel, el director de la unidad de carreteras de la provincia de Huesca y representantes del Ministerio de Obras Públicas españolas con resultados satisfactorios, el 18 de January de 2010. Se mantuvo un enlace de voz entre los dos nodos móviles a lo largo de un tramo de alrededor de 7.5 kilometros a una velocidad considerable. La voz resultó clara y sin interrupciones, lo que demuestra la validez del algoritmo de enrutamiento adaptado, la eficacia del algoritmo de entrega de los mensajes QoS y la validez del estudio previo que permitió el despliegue de la red. Parte de este trabajo fue enviado a la "International Conference on Wireless Communications in Underground and Confined Areas", mientras que los resultados completos se publicaron en la revista Ad Hoc Networks con el título "Real-time wireless multi-hop protocol in Underground Voice Communication".

La segunda aplicación experimental presentada en esta tesis ha sido la realización de una exploración real utilizando un equipo de robots controlados por operadores humanos, en el túnel de Somport. Este trabajo involucró distintos aspectos de robótica móvil como el control de movimiento, navegación y percepción cooperativa, localización y, por supuesto, la comunicación de tiempo real, teniendo en cuenta la características específicas del entorno. La aplicación consistia en llevar a cabo la tarea de explorar el túnel por un equipo de dos robots controlados por una estación base. El reto era realizar de manera semi-autónoma la exploración sin perder la conectividad de la red en ningún momento. El objetivo de alcanzar un refugio situado a una distancia considerable en ausencia de línea de visión entre la estación base y el robot de cabecera, y establecer una comunicación de voz y de video, fue completamente logrado. Esto fue posible mediante la implementación de un módulo de comunicación integrado en el sistema, capaz de manejar el tráfico de tiempo real, utilizado para el control de los robots, y el tráfico QoS para los flujos multimedia. Los resultados de este trabajo fueron presentados en el workshop ROBOT2011, celebrado en Sevilla en noviembre de 2011, con el título "Robot teams for exploration in underground environments".

La última aplicación presentada en esta tesis ha sido una novedosa técnica para planificar del despliegue de un equipo de varios robots a lo largo de un túnel, capaz de mantener en todo momento la conectividad de la red y aprovechar los los robots disponibles para llegar a la máxima cobertura en la exploración. La idea era tener en cuenta el análisis de la señal realizado en estos entornos y utiliza los parámetros de la señal para especializar la planificación. Por lo tanto, el robot líder utilizó la señal real medida en tiempo de ejecución para planificar su movimiento y el despliegue de los robots esclavos que, a la vez, actúavan como repetidores con la estación base. Este trabajo ha implicado varias contribuciones. En primer lugar, se ha desarrollado una técnica que utiliza los parámetros obtenidos por el análisis de la propagación de la señal para conducir el despliegue. En segundo lugar, se ha definido una estrategia general para este tipo de entorno en el que las señales presentan un comportamiento similar. Finalmente, el sistema completo se ha evaluó por medio de simulaciones y en un escenario real lo largo de tres kilómetros del túnel de Somport con resultados satisfactorios. Los resultados de esta contribución se publicarán en en número especiale sobre "Robotic Communications and Collaboration in Complex Environments" de la revista International Journal of Robotics Reserch (IJRR) con el titulo "Signal Based Deployment Planning for Robot Teams in Tunnel-like Fading Environments".

En resumen, en esta tesis doctoral hemos presentado un estudio completo sobre una plaforma inalámbrica de tiempo real que ofrece la posibilidad de gestión de los flujos con calidad de servicio al mismo tiempo. Ha sido desarrollado, probado extensivamente y mejorado en eficiencia, adaptando sus funcionalidades a la característica del entorno. La efectividad de la solución propuesta se se ha demostrado en aplicaciones reales en entornos subterráneos utilizado redes malladas y equipos multi robots.

Trabajo futuro

Hay varios frentes abiertos que requieren mejoras y un esfuerzo adicional.

Desde el punto de vista del protocolo, uno de retos principales es reducir la sobrecarga introducida por las distintas fases, que aumenta aún mas con la extensión QoS. Esta sobrecarga tiene una influencia en la escalabilidad del protocolo, que puede resultar limitada para redes de medio tamaño.

Un segundo reto seria completar la integración del mecanismo QoS en una arquitectura "cross-layer" con el sistema que la integra, para mejorar la eficiencia. Esto es posible mediante la adaptación de la carga de QoS, procedente de la capa de aplicación, a los recursos de red disponibles, estimados en tiempo de ejecución. Otra interesante mejora del mecanismo de QoS es añadir una técnica de "multicast" para permitir la comunicación entre los usuarios en el estilo de conferencia.

Desde el punto de vista del análisis de rendimiento, una limitación es la comparación con los protocolos presentes en la literatura, debido a que la gran mayoría de ellos se han propuesto y probado sólo en entornos de simulación. La implementación de nuestra solución en uno emulador de este tipo podría ser útil para demostrar su validez con respecto a otros protocolos.

Desde el punto de vista de la adaptación al entorno, sería necesario realizar más experimentos para tener una caracterización más general de la propagación de la señal. Por ejemplo, en nuestro trabajo no se tuvo en cuenta el impacto de los "fadings" transversales que podrían limitarse usando la propriedad de "diversity" de las antenas.

Appendix A

Field experiments

In this appendix we summarises some of field experiments conducted in outdoor and underground scenarios in the last four years. They dealt with topics primarily related to communications networking in MANETs and robot teams. Performance evaluation, mobility, signal propagation and network connectivity are some of topics applied to applications like multimedia communications, robot coperative navigation and wireless coverage.

A.1 Outdoor experiments

Cooperative robot navigation

RT-WMP protocol have been used to give network support to cooperation operations among robots. The cooperative navigation technique developed between 2008 and 2009 at RoPERT group motivated several experiments related with the protocol to share kinematic data among the members of the teams. This was used in the experiments carried out during the URUS project (see pictureA.1).

Figure A.1: Cooperative navigation at UPC.

PDR measurements

In order to characterize the PDR relation with respect the distance and the RSSI in a outdoor environment, we choose a field area quite free of obstacols (see picture A.2). The experiment testbed was composed by an emitting node based on a PcEngines ALIX3D3 board. This was equipped with an Atheros-based chipset wireless card and running a Linux operating system, programmed to emit broadcast frames periodically. The experiments were conducted at 2.142 GHz and 5.2 GHz frequencies.

Figure A.2: Outdoor PDR measurements.

RT-WMP versus OLSR mobility comparison

Most of valorable study about MANETs are interested on compare performances of different protocols. In our case, since the RT-WMP is an implemented protocol we performed a comparision with one of few implemented protocol presents in litterature, the OLSR protocol. To execute these experiments, we used the *unik-olsrd* implementation included in Ubuntu Linux 10.04 which supports natively the *link quality extension*. With these experiments, we evaluated the rough bandwidth offered and the mobility management by both protocols. The measurement was performed using four wireless nodes in a fixed position and a mobile one, represented by a robot, as shown in the picture A.3.

Figure A.3: RT-WMP vs OLSR mobility comparison tests.

A.2 Underground Experiments - Somport Tunnel

Mapping wireless coverage

Due to normal radio systems can provide at best a very limited communications capability in underground areas such as tunnel and mines, we started to investigate the propagation of wireless signal in these kind of environment. Many measurements was performedin order to characterize the propagation shape, following an empirical method. We took into account RSSI, PDR, delay spread.

Figure A.4: Mapping wireless coverage - Somport Tunnel

The experiment testbed was composed by an emitting node based on a PcEngines

ALIX3D3 board. This was equipped with an Atheros-based chipset wireless card and running a Linux operating system, programmed to emit broadcast frames periodically. We use as a mobile node a car expecially equipped for mobile test, with an odometer, laser (used localize any single measurement along the tunnel) and three laptop in charge of record the signal received. The experiments were conducted at 2.142 GHz and 5.2 GHz frequencies in the linear Somport tunnel and in the Santa Marta mine.

Figure A.5: Mapping wireless coverage - Santa Marta mine

Multimedia in Confined Environments

The main objectives of this experiments was to offer voice traffic support to mobile nodes in a confined environment. On May 2009 we started to investigate the electromagnetic propagation in these kind of environments. In a preliminary experiment (see picture A.6) we had evaluated the effect of a tunnel offer to the signal propagation as the multipath phenomena, delay spread and the waveguide behavior.

Figure A.6: First multimendia test at Somport tunnel

On September 2009 we carried out the first system experiment, using a total of seven node (see picture A.7). Five backbone nodes were deployed along about 4 kilometers, forming a chain network. Their relative position was fixed in order to maximaze the RSSI between them. Two laptops was used as mobile nodes, where was performing voice connection. This first test was not completely successful since voice communication was not fairly understandable.

Figure A.7: Preliminary experiments at the Somport Tunnel

After some adjustment and additional tests, a final experiment was successfully carried out on January 2010, in the presence of the director of road units and representatives of Ministry of public works (see picture A.8). Voice was transmitted perfectly between the two mobile nodes, without voice cuts and covering about 7 kilometers of the tunnel.

Figure A.8: Final test at Somport tunnel.

Robots team for autonomously exploration

In March 2009 we performed the first experiment where a team of mobile robots. was involved. The goal was to simulate a rescue/survellance operation using a robot In this scenario, the real-time multi-hop protocol RT-WMP supported the delay sensitive messages amongst nodes and the QoS extension was responsible for allowing end-to-end voice stream that allows the communication with possible victims. User voices were encoded in packets using the very efficient open source variable bit codec Speex [RFC5574 09], specifically designed for speech compression in VoIP applications.

Figure A.9: First and second test using a team of robot.

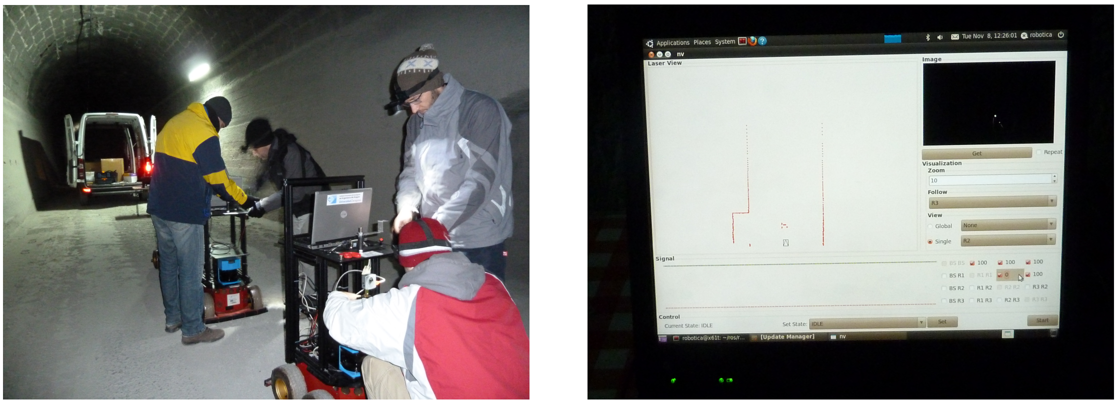


Figure A.10: Final test of autonomously exploration.

TCP/IP to MANET gateway

The main objectives of this experiments was to offer internet services in a confined environment. The experiment was carried out using a gateway between the RT-WMP and TCP/IP protocols in order to have access to internet services and get them available along the tunnel using the multihop network offered for the RT-WMP protocol.

We carried out a network of three nodes. The first was represented for a laptop and a mobile phone connected to the 3G network (see picture A.11). It was positioned near the entry of the tunnel where 3G network was available. The second one was a backbone node (as in the picture A.7) placed about one kilometer apart the first one. Finally, and the last one was a laptop used as a mobile node.

In order to validate the efectiveness of the network, we performed some test regarding the mobility (the last node was moving along the tunnel and maintaining connectivity) and on get available the internet services (like web surfing, chatting and skype call). Tests verify the effectiveness of the solution covering about 2 kilometer of tunnel.

Figure A.11: Laptop used as gateway and laptop used as mobile node along the tunnel.

Appendix B

The periods involved in the Blocking and Overhead protocol:

$$CT = T_{NEW\_TKN} + T_{EVALUATE\_TKN} + T_{SEND\_TKN}$$

$$\begin{aligned} ET &= T_{ISR} + T_{RECEIVE} + T_{DECODE\_RECEIVED} + \\ &+ T_{INTERPRET\_RECEIVED} + T_{EVALUATE\_TKN} + \\ &+ T_{SEND\_TKN} \end{aligned}$$

$$\begin{aligned} ETA &= T_{ISR} + T_{RECEIVE} + T_{DECODE\_RECEIVED} + \\ &+ T_{INTERPRET\_RECEIVED} + T_{EVALUATE\_TKN} + \\ &+ T_{CREATE\_AUTH} + T_{EVALUATE\_AUTH} + \\ &+ T_{SEND\_AUTH} \end{aligned}$$

$$\begin{aligned} EA &= T_{ISR} + T_{RECEIVE} + T_{DECODE\_RECEIVED} + \\ &+ T_{INTERPRET\_RECEIVED} + T_{EVALUATE\_AUTH} + \\ &+ T_{SEND\_AUTH} \end{aligned}$$

$$\begin{aligned} EME &= T_{ISR} + T_{RECEIVE} + T_{DECODE\_RECEIVED} + \\ &+ T_{INTERPRET\_RECEIVED} + T_{EVALUATE\_AUTH} + \\ &+ T_{CREATE\_MSG} + T_{EVALUATE\_MSG} + \\ &+ T_{SEND\_MSG} \end{aligned}$$

$$TH = \frac{header_{size} \cdot 8}{R}$$

$$\begin{aligned} EAM &= T_{ISR} + T_{RECEIVE} + T_{DECODE\_RECEIVED} + \\ &+ T_{INTERPRET\_RECEIVED} + T_{EVALUATE\_MSG} + \\ &+ T_{ENQUEUE\_MSG} \end{aligned}$$

Bibliography

[Abdrabou 06] A. Abdrabou & Weihua Zhuang. *A position-based QoS routing scheme for UWB mobile ad hoc networks.* Selected Areas in Communications, IEEE Journal on, vol. 24, no. 4, pages 850 – 856, april 2006.

[Aikio 98] P. Aikio, R. Gruber & P. Vainikainen. *Wideband radio channel measurements for train tunnels.* In Vehicular Technology Conference, 1998. VTC 98. 48th IEEE, volume 1, pages 460–464 vol.1, 1998.

[Aisa 10] J. Aisa & J.L. Villarroel. *WICKPro: A Hard Real-Time protocol for Wireless Mesh Networks with chain topologies.* In Wireless Conference (EW), 2010 European, pages 163 –170, april 2010.

[Akyildiz 05] I.F. Akyildiz & X. Wang. *A survey on wireless mesh networks.* Communications Magazine, IEEE, vol. 43, no. 9, pages S23 – S30, sept. 2005.

[Al-Karaki 04] J. N. Al-Karaki & J. M. Chang. *Quality of service support in IEEE 802.11 wireless ad-hoc networks.* Ad-hoc Networks, vol. 2, no. 3, pages 265–281, 2004.

[Alonso-Zarate 12] J. Alonso-Zarate, C. Crespo, Ch. Skianis, L. Alonso & Ch. Verikoukis. *Distributed point coordination function for IEEE 802.11 wireless ad hoc networks.* Ad Hoc Networks, vol. 10, no. 3, pages 536 – 551, 2012.

[Anastasi 04] G. Anastasi, E.Borgia, M.Conti & E. Gregori. *Wi-fi in ad hoc mode: a measurement study.* In in the Second IEEE Annual Conference on Pervasive Computing and Communications, pages 145 – 154, 2004.

[Andersen 02] S. V. Andersen, W.B. Kleijn, R. Hagen, J. Linden, M. N. Murthi & J. Skoglund. *iLBC - a linear predictive coder with robustness to packet losses.* In the 2002 IEEE Workshop on Speech Coding, pages 23–25, 2002.

[Aniss 04] H. Aniss, P.-M. Tardif, R. Ouedraogo & P. Fortier. *Communications network for underground mines based on the IEEE 802.11 and DOCSIS standards.* In Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, volume 5, pages 3605 – 3609 Vol. 5, 26-29 2004.

[Audsley 93] N. Audsley, A. Burns, M. Richardson, K. Tindell & A. J. Wellings. *Applying New Scheduling Theory to Static Priority Pre-Emptive Scheduling.* Software Engineering Journal, vol. 8, pages 284–292, 1993.

[Beaudoin 04] J.J. Beaudoin, G. Tran, P.-M. Tardif & P. Fortier. *Underground experiments of video transmission over an IEEE 802.11 infrastructure.* In Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, volume 5, pages 3610–3614 Vol. 5, Sept. 2004.

[Benzakour 04] A. Benzakour, S. Affes, C. Despins & P.M. Tardif. *Wideband measurements of channel characteristics at 2.4 and 5.8 GHz in underground mining environments.* In the 60th IEEE Vehicular Technology Conference, volume 5, pages 3595–3599, 2004.

[Canales 07] M. Canales, J. R. Gallego, A. Hernandez-Solana & A. Valdovinos. *Distributed Admission Control for Mobile Ad-Hoc Networks based on a Cross-layer Design.* Latin America Transactions, IEEE (Revista IEEE America Latina), vol. 5, no. 6, pages 425 –432, oct. 2007.

[Castellanos 99] J. A. Castellanos & J. D. Tardós. Kluwer Academic Publishers, Boston, MA, 1999.

[Chen 99] S. Chen & K. Nahrstedt. *Distributed quality-of-service routing in ad hoc networks.* IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pages 1488 – 1505, Aug., 1999.

[Damian 00] D. E. Herlea Damian, M. L. G. Shaw & B. R. Gaines. *Token-Passing Bus Access Method and Physical Layer Specifications.* IEEE Standard 802.4-1985, vol. 238, 2000.

[Dekker 96] D. Dekker, D. Hainsworth & W. McKeague. *Requirements for Underground Communications.* Mining Technology Conference, pages 102–109, Fremantle WA 1996.

[Delogne 82] P. Delogne. *Leaky Feeders and Subsurface Radio Communication.* IEE Electromagnetic waves, vol. 14, mar 1982.

[Dijkstra 59] E. W. Dijkstra. *A Note on Two Problems in Connexion with Graphs.* Numerische Mathematik, vol. 1, pages 269–271, 1959.

[Donatiello 03] L. Donatiello & M. Furini. *Ad-hoc Networks: A Protocol for Supporting QoS Applications.* In the 17th IEEE International Symposium on Parallel and Distributed Processing, pages 219–222, 2003.

[Dudley 07] D.G. Dudley, M. Lienard, S.F. Mahmoud & P. Degauque. *Wireless propagation in tunnels.* Antennas and Propagation Magazine, IEEE, vol. 49, no. 2, pages 11 –26, april 2007.

[Einicke 97] G. Einicke, D. Dekker & M. Gladwin. *A robust WLAN for survivable emergency communications.* In TENCON '97. IEEE Region 10 Annual Conference. Speech and Image Technologies for Computing and Telecommunications., Proceedings of IEEE, volume 1, pages 101 –104 vol.1, dec. 1997.

[Ergen 03] M. Ergen, D. Lee, R. Sengupta & P. Varaiya. *Wireless token ring protocol-performance comparison with IEEE 802.11.* Computers and Communication, 2003. (ISCC 2003). Proceedings. Eighth IEEE International Symposium on, pages 710–715 vol.2, July 2003.

[Eth 05] *IEEE Std 802.3 - 2005 Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.* IEEE Std 802.3-2005 (Revision of IEEE Std 802.3-2002 including all approved amendments), vol. Section1, pages 1 – 594, 2005.

[Facchinetti 05] T. Facchinetti, G. Buttazzo & L. Almeida. *Dynamic resource reservation and connectivity tracking to support real-time communication among mobile units.* EURASIP Journal on Wireless Communication and Networking, vol. 5, no. 5, pages 712–730, 2005.

[FDD 98] *ANSI FDDI Standard - Physical Layer Protocol (PHY).* American National Standards Institute, vol. ANSI Std. X3.148-1998, ISO 9314-1:1989, 1998.

[Fink 10] J. Fink & V. Kumar. *Online methods for radio signal mapping with mobile robots.* In IEEE International Conference on Robotics and Automation, pages 1940–1945, May Anchoragei,2010.

[FIP 90] FIP. *FIP Bus for Exchange of Information Between Transmitters.* In French Association for Standardization, NF C46 601-607, 1990.

[Goldsmith 05] A. Goldsmith. Wireless communications. Cambridge University Press, 2005.

[Grow 82] R. Grow. *A timed token protocol for local area networks.* In Electro, page Paper 17/3, May 1982.

[Hamidian 07] A. Hamidian & U. Körner. *Providing QoS in Ad Hoc Networks with Distributed Resource Reservation.* In 20th International Teletraffic Congress (ITC-20), 2007, Ottawa, Canada, June 2007.

[Hanzo-II 07] L. Hanzo-II & R. Tafazolli. *A SURVEY OF QOS ROUTING SOLUTIONS FOR MOBILE AD HOC NETWORKS.* Communications Surveys Tutorials, IEEE, vol. 9, no. 2, pages 50 –70, quarter 2007.

[Holland 01] G. Holland, N. Vaidya & P. Bahl. *A rate-adaptive MAC protocol for multi-Hop wireless networks.* In Proceedings of the 7th annual international conference on Mobile computing and networking, MobiCom '01, pages 236–251, New York, NY, USA, 2001. ACM.

[Hsieh 08] M. Ani Hsieh, Anthony Cowley, Vijay Kumar & Camillo J. Taylor. *Maintaining network connectivity and performance in robot teams.* Journal of Field Robotics, vol. 25, no. 1-2, pages 111–131, 2008.

[Hung-Yu 06] W. Hung-Yu, K. Kyungtae, A. Kashyap & S. Ganguly. *On Admission of VoIP Calls Over Wireless Mesh Network.* In Communications, 2006. ICC '06. IEEE International Conference on, volume 5, pages 1990 –1995, june 2006.

[Hwang 98] Y. Hwang, Y.P. Zhang & R.G. Kouyoumjian. *Ray-optical prediction of radio-wave propagation characteristics in tunnel environments. 1. Theory.* Antennas and Propagation, IEEE Transactions on, vol. 46, no. 9, pages 1328 –1336, sep 1998.

[IEEE 97] IEEE. *Standards for Local and Metropolitan Area Networks: Supplement to Token-Passing Bus Access Method and Physical Layer Specifications. Alternative Use of BNC Connectors and Manchester-Encoded Signaling Methods for Single-Channel Bus Physical Layer Entities.* IEEE Std 802.4h-1997, 1997.

[IEEE 05] IEEE. *802.11e-2005 Standard, Part 11e: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements.* IEEE Computer Society LAN MAN Stradards Committee, 2005.

[IEEE 07] IEEE. *IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), pages 1 –1076, 12 2007.

[ISO 93] ISO. *Road Vehicles - Interchange of Digital Information - Controller Area Network (CAN) for High-Speed Communication.* International Standards Organisation, 1993.

[ITU-T 99] ITU-T. *Definition of Categories of Speech Transmission Quality.* In ITU-T Recommendation G.109, Geneva, 1999.

[ITU-T 03] ITU-T. *One-way transmission time.* In ITU-T Recommendation G.114, May 2003.

[Jacquet 03] P. Jacquet, P. Muhlethaler, A. Qayyum, A. Laouiti, L. Viennot & T. Clausen. *RFC 3626 - Optimized Link State Routing Protocol (OLSR).* Internet Engineering Task Force, 2003.

[Jun 03] J. Jun, P. Peddabachagari & M. Sichitiu. *Theoretical Maximum Throughput of IEEE 802.11 and its Applications.* In the 2nd IEEE International Symposium on Network Computing and Applications, page 249, 2003.

[Kopetz 89] H. Kopetz, A. Damm, C. Koza, M. Mulazzani, W. Schwabl, C. Senft & R. Zainlinger. *Distributed fault-tolerant real-time systems: the Mars approach.* IEEE Micro, vol. 9, pages 25–40, Feb. 1989.

[Kosek-Szott 12] K. Kosek-Szott. *A survey of MAC layer solutions to the hidden node problem in ad-hoc networks.* Ad Hoc Networks, vol. 10, no. 3, pages 635 – 660, 2012.

[Lazaro 10] M.T. Lazaro & J.A. Castellanos. *Localization of probabilistic robot formations in SLAM.* In Robotics and Automation (ICRA), 2010 IEEE International Conference on, pages 3179 –3184, may 2010.

[Le Lann 93] G. Le Lann & N. Riviere. *Real-Time communications over broadcast networks: the CSMA-DCR and the DOD-CSMA-CD protocols*. Rapport technique, INRIA, 1993.

[Lee 02] D. Lee, R. Attias, A. Puri, R. Sengupta, S. Tripakis & P. Varaiya. *A Wireless Token Ring Protocol For Ad-Hoc Networks*. In the 2002 Aerospace Conference, 2002.

[Lienard 98] M. Lienard & P. Degauque. *Propagation in wide tunnels at 2 GHz: a statistical analysis*. IEEE Transactions on Vehicular Technology, vol. 47, no. 4, pages 1322 –1328, nov 1998.

[Lienard 99] M. Lienard, S. Betrencourt & P. Degauque. *Theoretical and experimental approach of the propagation at 2.5 GHz and 10 GHz in straight and curved tunnels*. In Vehicular Technology Conference, 1999. VTC 1999 - Fall. IEEE VTS 50th, 1999.

[Lienard 00] M. Lienard & P. Degauque. *Natural wave propagation in mine environments*. Antennas and Propagation, IEEE Transactions on, vol. 48, no. 9, pages 1326–1339, Sep 2000.

[Lin 97] C.R. Lin & M. Gerla. *Asynchronous multimedia multihop wireless networks*. INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, vol. 1, pages 118–125 vol.1, Apr 1997.

[Liu 73] C. L. Liu & James W. Layland. *Scheduling Algorithms for Multiprogramming in a Hard-Real-Time Environment*. In Journal of ACM, volume 20, pages 46–61, 1973.

[Malcolm 94] N. Malcolm & W. Zhao. *The Timed-Token Protocol for Real-Time Communications*. Computer, vol. 27, no. 1, pages 35–41, Jan. 1994.

[Malcolm 95] N. Malcolm & W. Zhao. *Hard real-time communication in multiple-access networks*. Real-Time Systems, vol. 8, no. 1, pages 35–77, 1995.

[Mangold 02] S. Mangold, S. Choi, P. May, O. Klein, G. Hiertz & L. Stibor. *IEEE 802.11e Wireless LAN for Quality of Service*. In the European Wireless, pages 32–39, 2002.

[Martínez 03] J. M. Martínez, M. González Harbour & J. J. Gutiérrez. *RT-EP: Real-Time Ethernet Protocol for Analyzable Distributed Applications on a Minimum Real-Time POSIX Kernel*. In Proceedings of the 2nd International Workshop on Real-Time LANs in the Internet Age, 2003.

[Martínez 05] J. M. Martínez & M. González Harbour. *RT-EP: A Fixed-Priority Real Time Communication Protocol over Standard Ethernet.* In the 10th International Conference on Reliable Software Technologies, Ada-Europe, pages 180–195, 2005.

[Masson 09] E. Masson, P. Combeau, M. Berbineau, R. Vauzelle & Y. Pousset. *Radio Wave Propagation in Arched Cross Section Tunnels - Simulations and Measurements.* Journal of Communications, vol. 4, no. 4, pages 276–283, 2009.

[Minguez 01] J. Minguez, L. Montano, T. Simeon & R. Alami. *Global Nearness Diagram Navigation (GND).* In IEEE Int. Conf. on Robotics and Automation (ICRA'01), pages 33–39, 2001.

[Minguez 04] J. Minguez & L. Montano. *Nearness diagram (nd) navigation: Collision avoidance in troublesome scenarios.* IEEE Transactions on Robotics and Automation, vol. 20, no. 1, pages 45–59, 2004.

[Minguez 05] J. Minguez. *The Obstacle-Restriction Method (ORM) for Robot Obstacle Avoidance in Difficult Environments.* In Proc. of the IEEE Int. Conf. on Intelligent Robots and Systems, page 37063712, 2005.

[Molisch 11] A. F. Molisch. Wireless Communications. Wiley-IEEE press, 2011.

[Molle 85] M. Molle & L. Kleinrock. *Virtual time CSMA: Why two clocks are better than one.* IEEE Transaction Commununication, vol. 33, pages 919–933, Sep. 1985.

[Moutairou 06] M. Moutairou, H. Aniss & G. Y. Delisle. *Wireless mesh access point routing for efficient communication in underground mine.* In the 2006 IEEE Antennas and Propagation Society International Symposium, pages 577–580, 2006.

[Multimedia 11] Multimedia. `http://robots.unizar.es/html/ficha_resultado.php?id=74`, 2011.

[Multimedia 12] Multimedia. `http://robots.unizar.es/html/ficha_resultado.php?id=158&idmember=`, 2012.

[Murphy 08] R. R. Murphy, R. Shoureshi, H. W. Arnold, H. Arslan, J. Burke, L. J. Greenstein, D. K. Killinger, C. W. Lundgren, A. J. Rustako & S. Stover. *Analysis of Viability and Feasibility of Current and Emerging Mining Communication and Mine*

Rescue Technologies. In Institute for Safety, Security, Rescue Technology, University of South Florida, Final Report, March 2008.

[Nakamura 96] N. Nakamura, H. Tsunomachi & R. Fukui. *Road vehicle communication system for vehicle control using leaky coaxial cable*. Comm. Mag., vol. 34, no. 10, pages 84–89, October 1996.

[Nerguizian 05] C. Nerguizian, C.L. Despins, S. Affes & M. Djadel. *Radio-channel characterization of an underground mine at 2.4 GHz*. Wireless Communications, IEEE Transactions on, vol. 4, no. 5, pages 2441–2453, Sept. 2005.

[Ng 07] P. C. Ng & S.C. Liew. *Throughput Analysis of IEEE 802.11 Multi-hop Ad-hoc Networks*. IEEE/ACM Transaction on Networking , 2007.

[Nguyen 04] H. G. Nguyen, N. Pezeshkian, A. Gupta & N. Farrington. *Maintaining Communication Link for a Robot Operating in a Hazardous Environment*. In the 10th International Conference on Robotics and Remote Systems for Hazardous Environments, 2004.

[NS2 11] NS2. *Network simulator v.2*. `http://www.isi.edu/nsnam/ns/`, 2011.

[OMNeT 12] OMNeT. `http://www.omnetpp.org/`, 2012.

[Opnet 12] Opnet. `http://www.opnet.com/`, 2012.

[PBUS 96] PBUS. *EN 50170, General Purpose Field Communication System, Volume 2/3 (PROFIBUS)*. CENELEC, 1996.

[Peasgood 06] M. Peasgood, J. McPhee & C. Clark. *Complete and Scalable Multi-robot Planning in Tunnel Environments*. In 1st IFAC Workshop on Multivehicle Systems, October 2006.

[Perkins 94] C. E. Perkins & P. Bhagwat. *Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers*. In Proceedings of the conference on Communications architectures, protocols and applications, SIGCOMM '94, pages 234–244, New York, NY, USA, 1994. ACM.

[Perkins 03] C. Perkins, E. Royer & S. Das. *RFC 3561 - Ad-hoc On-Demand Distance Vector (AODV) Routing*. Internet Engineering Task Force, 2003.

[Pojda 11] J. Pojda, A. Wolff, M. Sbeiti & C. Wietfeld. *Performance analysis of mesh routing protocols for UAV swarming applications.* In Wireless Communication Systems (ISWCS), 2011 8th International Symposium on, pages 317 –321, nov. 2011.

[Pop 06] T. Pop, P. Pop, P. Eles, Z. Peng & A. Andrei. *Timing analysis of the FlexRay communication protocol.* In Real-Time Systems, 2006. 18th Euromicro Conference on, pages 11 pp. –216, 0-0 2006.

[Pradhan 98] P. Pradhan & T. Chiueh. *Real-Time Performance Guarantees over Wired/Wireless LANs.* In the 4th IEEE Real-Time Technology and Applications Symposium, pages 29–38, 1998.

[Qin 06] L. Qin & T. Kunz. *Mobility Metrics to Enable Adaptive Routing in MANET.* In Wireless and Mobile Computing, Networking and Communications, 2006. (WiMob'2006). IEEE International Conference on, pages 1 –8, june 2006.

[Quigley 09] M. Quigley, K. Conley, B. P. Gerkey, J. Faust, T. Foote, J. Leibs, R. Wheeler & A. Y. Ng. *ROS: an open-source Robot Operating System.* In ICRA Workshop on Open Source Software, 2009.

[Ramamritham 94] K. Ramamritham & J. A. Stankovic. *Scheduling Algorithms and Operating Systems Support for Real-Time Systems.* In Proceedings of the IEEE, volume 82, pages 55–67, 1994.

[Ramanathan 02] R. Ramanathan & J. Redi. *A brief overview of ad hoc networks: challenges and directions.* Communications Magazine, IEEE, vol. 40, no. 5, pages 20 –22, may 2002.

[Rappaport 96] T. S. Rappaport. Wireless communications. Principles and Practice. Prentice Hall, 1996.

[Ray 03] S. Ray, J. B. Carruthers & D. Starobinski. *RTS/CTS-induced congestion in ad-hoc wireless LANs.* In the 2003 Wireless Communications and Networking Conference, volume 3, pages 1516–1521, 2003.

[Reddy 06] T. B. Reddy, I. Karthigeyan, B. S. Manoj & C. S. Murthy. *Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions.* Ad Hoc Netw., vol. 4, no. 1, pages 83–124, January 2006.

[Reddy 07] T. Bheemarjuna Reddy, John P. John & C. Siva Ram Murthy. *Providing MAC QoS for multimedia traffic in 802.11e based multi-hop ad hoc wireless networks.* Comput. Netw., vol. 51, no. 1, pages 153–176, 2007.

[RFC5574 09] RFC5574. *RTP Payload Format for the Speex Codec.* Internet Engineering Task Force, 2009.

[Rivas 01] M. Aldea Rivas & M. González Harbour. *MaRTE OS: An Ada Kernel for Real-Time Embedded Applications.* In In Proceedings of the 6th International Conference on Reliable Software Technologies, Ada-Europe-2001, 2001.

[Rizzo 13] C. Rizzo, D. Tardioli, D. Sicignano, L. Riazuelo, J. L. Villarroel & L. Montano. *Signal Based Deployment Planning for Robot Teams in Tunnel-like Fading Environments.* The International Journal of Robotics Research - Awaiting publication, 2013.

[Schwarz 02] M. Schwarz. Implementation of a TTP/C Cluster Based on Commercial Gigabit Ethernet Components. Master's thesis, Technische Universität Wien, Institut für Technische Informatik, Vienna, Austria, 2002.

[Seidel 94] S.Y. Seidel & T.S. Rappaport. *Site-specific propagation prediction for wireless in-building personal communication system design.* IEEE Transactions on Vehicular Technology, vol. 43, no. 4, pages 879 –891, nov 1994.

[Sheu 04] J. P. Sheu, C. H. Liu, S. L. Wu & Y. C. Tseng. *A priority MAC protocol to support real-time traffic in ad-hoc networks.* Wireless Networks, vol. 10, no. 1, pages 61–69, Jan. 2004.

[Sicignano 10a] D. Sicignano, D. Tardioli & J. L. Villarroel. *QoS over Real Time wireless multihop Network.* In Ad Hoc Networks, volume 28 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 110–128, 2010.

[Sicignano 10b] D. Sicignano, D. Tardioli & J. L. Villarroel. *QoS over Real Time wireless multihop Network.* In J. Zheng et al. (Eds.): AD-HOCNETS 2009, LNICST, volume 28, pages 110–128, 2010.

[Sicignano 10c] D. Sicignano, D. Tardioli & J. L. Villarroel. *RT-WMP in Underground Voice Communication.* In the 3rd International Conference on Wireless Communications in Underground and Confined Areas, 2010.

[Sicignano 11] D. Sicignano, D. Tardioli, S. Cabrero & J. L. Villarroel. *Real-time wireless multi-hop protocol in underground voice communication.* Ad Hoc Networks, no. doi: 10.1016/j.adhoc.2011.01.017, 2011.

[Sobrinho 96] J. L. Sobrinho & A.S. Krishnakumar. *Real-Time Traffic over the IEEE 802.11 Medium Access Control Layer.* Bell Labs Technical Journal, vol. 1, no. 2, pages 172–87, 1996.

[Sobrinho 98] J. L. Sobrinho & A. S. Krishnakumar. *EQuB-Ethernet quality of service using black bursts.* In the 23rd Annual Conference on Local Computer Networks, pages 286–296, 1998.

[Sobrinho 99] J. L. Sobrinho & A.S. Krishnakumar. *Quality-of-service in ad-hoc carrier sense multiple access wireless networks.* IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pages 1353–1368, Aug. 1999.

[Souryal 06] M. R. Souryal, L. Klein-Berndt, L.E. Miller & N. Moayeri. *Link Assessment in an Indoor 802.11 Network.* In the 2006 IEEE Wireless Communications & Networking Conference, 2006.

[Srinivasan 06] K. Srinivasan & P. Levis. *RSSI is Under Appreciated.* In Proceedings of the Third Workshop on Embedded Networked Sensors (EmNets), 2006.

[Stankovic 04] J. A. Stankovic. *Research Challenges for Wireless Sensor Networks.* SIGBED Review: Special Issue on Embedded Sensor Networks and Wireless Computing, vol. 1, no. 2, pages 9–12, July 2004.

[Sun 10] Z. Sun & I.F. Akyildiz. *Channel modeling and analysis for wireless networks in underground mines and road tunnels.* IEEE Transactions on Communications, vol. 58, no. 6, pages 1758 –1768, june 2010.

[Suthakorn 09] J. Suthakorn, S.S.H. Shah, S. Jantarajit, W. Onprasert, W. Saensupo, S. Saeung, S. Nakdhamabhorn, V. Sa-Ing & S. Reaungamornrat. *On the design and development of a rough terrain robot for rescue missions.* In Robotics and Biomimetics, 2008. ROBIO 2008. IEEE International Conference on, pages 1830 –1835, feb. 2009.

[Szott 09] S. Szott, M. Natkaniec & A. Banchs. *Impact of Misbehaviour on QoS in Wireless Mesh Networks.* In Luigi Fratta, Henning

Schulzrinne, Yutaka Takahashi & Otto Spaniol, editeurs, NETWORKING 2009, volume 5550 of *Lecture Notes in Computer Science*, pages 639–6502. Springer Berlin Heidelberg, 2009.

[Taheri 02] S.A. Taheri & A. Scaglione. *Token enabled multiple access (TEMA) for packet transmission in high bit rate wireless local area networks*. Communications, 2002. ICC 2002. IEEE International Conference on, vol. 3, pages 1913–1917 vol.3, 2002.

[Tanabe 11] S. Tanabe, K. Sawai & T. Suzuki. *Sensor Node Deployment Strategy for Maintaining Wireless Sensor Network Communication Connectivity*. International Journal of Advanced Computer Science and Applications (IJACSA), vol. 2, no. 12, pages 140–146, 2011.

[Tanenbaum 97] A. S. Tanenbaum. Computers networks. Prentice-Hall, Inc., 1997.

[Tanenbaum 06] A. S. Tanenbaum & M. Steen. Distributed systems: Principles and paradigms (2nd edition). Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2006.

[Tardioli 07] D. Tardioli & J.L. Villarroel. *Real Time Communications over 802.11: RT-WMP*. Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on, pages 1–11, Oct. 2007.

[Tardioli 10] D. Tardioli, A. R. Mosteo, L. Riazuelo, J. L. Villarroel & L. Montano. *Enforcing Network Connectivity in Robot Team Missions*. The International Journal of Robotics Research, vol. 29, no. 4, pages 460 – 480, Apr. 2010.

[Tardioli 11] D. Tardioli, D. Sicignano, L. Riazuelo, J. L. Villarroel & L. Montano. *Robot teams for exploration in underground environments*. In in Proceedings of the Workshop ROBOT2011, November 2011.

[Tardioli 12a] D. Tardioli. *ros-rt-wmp*. `http://www.ros.org/wiki/ros-rt-wmp`, 2012.

[Tardioli 12b] D. Tardioli & J.L. Villarroel. *Routing wireless real-time traffic using minimum spanning trees*. In Computing, Networking and Communications (ICNC), 2012 International Conference on, pages 170 –176, 30 2012-feb. 2 2012.

[Tardioli 13] D. Tardioli, D. Sicignano & J. L. Villarroel. *A Wireless Multi-hop Protocol for Real-Time Applications*. Ad Hoc Networks - Under Revision, 2013.

[Tindell 94] K. Tindell & J. Clark. *Holistic schedulability analysis for distributed hard real-time systems*. Microprocessing and Microprogramming, vol. 40, no. 2-3, pages 117 – 134, 1994.

[Urcola 09] P. Urcola & L. Montano. *Cooperative robot team navigation strategies based on an environment model*. In the 2009 IEEE International Conference on Intelligent Robots and Systems, pages 4577–4583, 2009.

[Venkatramani 94] C. Venkatramani & Tzi cker Chiueh. *Supporting real-time traffic on Ethernet*. In the 15th Real-Time Systems Symposium, pages 282–286, 1994.

[Vlaovic 01] B. Vlaovic & Z. Brezocnik. *Packet based telephony*. EUROCON'2001, Trends in Communications, International Conference on., vol. 1, pages 210–213 vol.1, 2001.

[Vlavianos 08] A. Vlavianos, L.K. Law, I. Broustis, S.V. Krishnamurthy & M. Faloutsos. *Assessing link quality in IEEE 802.11 Wireless Networks: Which is the right metric?* In Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on, pages 1–6, Sept. 2008.

[Wadhwa 11] A. Wadhwa, U. Madhow, J. Hespanha & B.M. Sadler. *Following an RF trail to its source*. In Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on, pages 580 –587, sept. 2011.

[Walker 09] V. Walker. *Idaho National Laboratory*. `https://inlportal.inl.gov/portal/server.pt?open=514&objID=1269&mode=2&featurestory=DA_325880`, 2009.

[Wang 01] Y. Wang & B. Bensaou. *Achieving fairness in IEEE 802.11 DFWMAC with variable packet lengths*. Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE, vol. 6, pages 3588–3593 vol.6, 2001.

[Wang 05] M. Wang & G. Kuo. *An application-aware qos routing scheme with improved stability for multimedia applications in mobile ad hoc networks*. In Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd, volume 3, pages 1901 – 1905, Sept., 2005.

[Wang 06] J. Wang, X. Zhu & J. Chen. *Link Availability at Any Time in MANET*. In T. Kunz & S.S. Ravi, editeurs, Ad-Hoc, Mobile, and Wireless Networks, volume 4104 of *Lecture Notes in Computer Science*, pages 184–196. Springer Berlin Heidelberg, 2006.

[Wang 07] P. Wang & W. Zhuang. *A Token-Based Scheduling Scheme for WLANs and Its Performance Analysis*. In the 2007 IEEE International Conference on Communications, 2007. ICC '07., pages 3716–3721, 2007.

[White 10] C. White, D. Hiranandani, C. S. Olstad, K. Buhagiar, T. Gambin & C. M. Clark. *The Malta cistern mapping project: Underwater robot mapping and localization within ancient tunnel systems*. J. Field Robot., vol. 27, no. 4, pages 399–411, July 2010.

[Wu 08] D. Wu, P. Djukic & P. Mohapatra. *Determining 802.11 link quality with passive measurements*. In the 2008 IEEE International Symposium onWireless Communication Systems, pages 728 –732, 2008.

[Yan 08] Z. Yan, W. Dapeng, W. Bin, W. Muqing & X. Chunxiu. *A Novel Call Admission Control Routing Mechanism for 802.11e Based Multi-Hop MANET*. In Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on, pages 1 –4, oct. 2008.

[Yan 12] Y. Yan & Y. Mostofi. *Robotic Router Formation in Realistic Communication Environments - A Bit Error Rate Approach*. IEEE Transactions on Robotics, 2012.

[Yang 05] X. Yang & N. Vaidya. *On physical carrier sensing in wireless ad hoc networks*. In the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, volume 4, pages 2525 – 2535, 2005.

[Yarkan 08] S. Yarkan, S. Guzelgoz & H. Arslan. *Wireless Channel Propagation Characteristics in Underground Mines: A Statistical Analysis and A Radio Controlled Robot Experiment*. In Proc. second IEEE International Conference on Wireless Communications in Underground and Confined Areas (ICWCUCA), Aug. 2008.

[Yarkan 09] S. Yarkan, S. Guzelgoz, H. Arslan & R.R. Murphy. *Underground Mine Communications: A Survey*. Communications

Surveys & Tutorials, IEEE, vol. 11, no. 3, pages 125–142, Quarter 2009.

[Ye 01] H. Ye, G. C. Walsh & L. Bushnell. *Real-Time Mixed Traffic Wireless Networks.* IEEE Transactions on Industrial Electronics, vol. 8, no. 5, Oct. 2001.

[Yigitbasi 08] N. Yigitbasi & F. Buzluca. *A control plane for prioritized real-time communications in wireless token ring networks.* In Computer and Information Sciences, 2008. ISCIS '08. 23rd International Symposium on, pages 1–6, oct. 2008.

[Zhai 06] H. Zhai, J. Wang & Y. Fang. *DUCHA: A New Dual-Channel MAC Protocol for Multihop Ad Hoc Networks.* Wireless Communications, IEEE Transactions on, vol. 5, no. 11, pages 3224–3233, November 2006.

[Zhang 06] X. Zhang, L. Tan, J. Li, S. Zhao & H. Chen. *Active-time Based Bandwidth Allocation for Multi-hop Wireless Ad Hoc Networks.* In Communications, 2006. ICC '06. IEEE International Conference on, volume 8, pages 3789 –3794, june 2006.

[Zhang 08] J. Zhang, K. Liu & X. Shen. *A Novel Overlay Token Ring Protocol for Inter-Vehicle Communication.* Communications, 2008. ICC '08. IEEE International Conference on, pages 4904–4909, May 2008.

[Zhuang 08] F. Zhuang, C. Zupan, Z. Chao & Z. Yanzheng. *A cable-tunnel inspecting robot for dangerous environment.* vol. 5, no. 3, pages 243–248, 2008.

Acronyms

ATP	Authorization Transmission Phase
BEB	Binary Exponential Back-Off
BER	Bit Error Rate
CDMA	Code Division Multiple Access
CSMA	Carrier-Sense Multiple Access
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DCF	Distributed Coordination Function
EABW	Estimated Available Bandwidth
EDCA	Enhanced Distributed Channel Access
EDF	Enhanced Distributed Function
E2E	End-to-End Delay
FAC	Flow Admision Control
FDDI	Fiber Distributed Data Interface
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
IAT	Inter-Arrival Time
LF	Leaky Feeder
LoS	Line-of-Sight
LQM	Link Quality Matrix

LRT	Loop Remaining Time
MANET	Mobile Ad-Hoc Network
MAC	Medium Access Control
MOS	Mean Opinion Score
MTP	Message Transmission Phase
ND	Nearness Diagram
ND-HS	Nearness Diagram High Speed
OLSR	Optimized Link State Routing
ORM	Obstacle-Restriction Method
PAP	Priority Arbitration Phase
PCF	Point Coordination Function
PDR	Packet Delivery Ratio
QoS	Quality of Service
RSSI	Receive Signal Strength Indication
RT-WMP	Real Time Wireless Multihop Protocol
SINR	Signal to Interference plus Noise Ratio
SNR	Signal to Noise Ratio
TDMA	Time Division Multiple Access
TMT	Theoretical Maximum Throughput
TTE	Through-the-Earth
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network