Experiments with OLSR Routing in a MANET

Cédric Adjih[1], **Pascale Minet**[1], **Thierry Plesse**[2], **Anis Laouiti**[1], **Adokoe Plakoo**[1], **Marc Badel**[1], **Paul Mühlethaler**[1], **Philippe Jacquet**[1], **and Jérome Lecomte**[2]
[1]INRIA, BP 105, Rocquencourt, 78153 Le Chesnay Cedex, France.
[2]DGA/CELAR, BP 7419, 35174 Bruz Cedex, France.

email: {cedric.adjih|pascale.minet|anis.laouiti|adokoe.plakoo|marc.badel}@inria.fr
{paul.muhlethaler|philippe.jacquet}@inria.fr / {plesse|lecomte}@celar.fr

Abstract

Wireless ad-hoc networks (MANETs) are autonomous, self-configuring and adaptive networks. Their ability to adapt themselves to dynamic, random and rapidly changing multihop topologies is given by a multihop routing protocol. In this paper, we describe experiments made with a real MANET consisting of 18 nodes implementing the OLSR routing protocol operating over radio with IEEE 802.11 hardware. More precisely, we report measurements that were made in the areas of (i) the speed of deployment, (ii) the adaptability to topology changes, (iii) the mobility support, and (iv) the dependability. Measures show that a MANET equipped with OLSR routing meets most requirements of future applications such as rescue applications or military tactical applications in urban context.

1 Introduction

Mobile Ad-hoc Networks (MANETs) enjoy a rising interest and are becoming more and more popular. The reason of this interest can be explained by many advantages of MANETs, in parallel with the success of wireless technologies. Wireless ad-hoc networks are autonomous, self-configuring and self-adaptive networks. Their ability to be operational rapidly and without any preexisting infrastructure is appreciated in rescue applications or more generally in applications operating in changing, unstable or hostile environment... Moreover, they adapt themselves to dynamic, random and rapidly changing multihop topologies. To achieve that, a routing protocol is needed. This protocol can automatically discover the neighbors and topology, and sets up routes. Such networks also support mobility, as the information about routes and topology is constantly updated. MANETs can also support different types of user traffic: voice, video and data. As they do not require any centralized control, their dependability is good. Such networks can be connected, if needed, to a fixed network and to other MANETs. Their evolutivity allows the insertion of new nodes. Thus, MANETs are excellent candidates for intelligent transportation systems, military tactical networks, where their ability to be operational rapidly and without any centralized entity is essential.

Adjih, C.; Minet, P.; Plesse, T.; Laouiti, A.; Plakoo, A.; Badel, M.; Mühlethaler, P.; Jacquet, P.; Lecomte, J. (2006) Experiments with OLSR Routing in a MANET. In *Military Communications* (pp. 23-1 – 23-24). Meeting Proceedings RTO-MP-IST-054, Paper 23. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Experiments with OLSR Routing in a MANET	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **INRIA, BP 105, Rocquencourt, 78153 Le Chesnay Cedex, France**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202750. RTO-MP-IST-054, Military Communications (Les communications militaires), The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**24**	

The purpose of this paper is to provide a quantitative evaluation of the behavior of a real MANET comprising eighteen nodes implementing OLSR (Optimized Link State Routing) protocol operating with the IEEE 802.11b equipement over a radio channel. In particular, we will focus on four criteria corresponding to the first four advantages previously listed: (i) the speed of deployment, (ii) the adaptability to topology changes, (iii) the mobility support, and (iv) the dependability. This paper is organized as follows. Section 2 explains why MANETs must be considered in tactical networks of the armed forces. In Section 3, after a brief presentation of the OLSR routing protocol, we describe the MANET/OLSR platform we have built and installed. Section 4 reports the results, obtained by means of measurements, with regard to each given criterium. Finally, we conclude.

2 Network Centric Warfare

For several years, the concepts of ”battlefield numerisation” and ”Network Centric Warfare” (NCW), have made information control a determining stake for the armed forces. NCW doctrine integrates all the tactical components : warriors, Unmanned Ground Vehicules (UGV), Unmanned Aerial Vehicules (UAV), tactical vehicules, command vehicules, tanks,... This concept requires an architecture of meshed network, adapting automatically to variable topologies. Such a network performs auto-configuration, and dynamic routing. It detects the presence of a new node, the absence of another one and supports nodes mobility. Networks meeting, wholly or partly, these requirements are under development in the civil world: Mobile Ad-hoc NETworks (MANETs).

The convergence of the Internet Revolution, which has brought the IP protocol to maturity on the civilian market, and the increasing needs of interoperability for data transmission architectures on the battlefield for joint and allied forces has made the use of COTS technologies and products in Telecommunications protocols a major issue for Defense C4I (Command, Control, Communications, Computers and Information) systems. The effort known as MANET (Mobile Ad-hoc NETwork), led by the Internet Engineering Task Force (IETF), to bring new promising answers to technical issues raised by mobile context about IP network, specifically relative to availability and reliability, is of great interest for military applications.

In military scenarios, nothing can ensure that all communicating nodes are one-hop away due to the inherent nature of the radio propagation. In that case, ad-hoc multihop architecture is one of the best approaches to solve the connectivity problem. An architecture with a distributed control is essential and centralized functions should be limited to optimization capabilities. Autonomous packet radio networks are essential because of their ability to be operational rapidly and without any infrastructure. Military requirements and constraints make MANET more pertinent relatively to the Below of Brigade echelon.

3 MANET/OLSR Platform

3.1 OLSR Presentation

As radio coverage is usually limited, multihop routing is generally needed. The IETF MANET (Mobile Ad-hoc NETwork) working group aims at standardizing dynamic routing in ad-hoc networks. All the routing protocols proposed in the MANET group address the problem of unicast routing, while taking into account the features of wireless, multihop, mobile ad-hoc networks. Such protocols can be divided into two classes: proactive and reactive, depending on the route establishment mechanism that is used.

With reactive protocols, a node discovers routes on-demand and maintains only active ones. Thus, a route

is discovered whenever a source node needs to communicate with a destination node for which a route is not available. This discovery mechanism is based on pure flooding [1] in the network. Two reactive protocols are on the standard track or established RFCs: AODV [2] and DSR [3].

OLSR (Optimized Link State Routing) [8] is a proactive routing protocol that is now an RFC. It provides the advantage of having routes immediately available in each node for all destinations in the network. Periodic control packets are in charge of monitoring the network topology. This class of protocol is particularly well suited for applications where all nodes can use the topology knowledge discovered by the routing protocol. Moreover, proactive routing protocols can be used without modification in the network protocol stack.

OLSR is an optimization of a pure link state routing protocol. It is based on the concept of *multipoint relays* (*MPRs*) [9]. First, using *multipoint relays* reduces the size of the control messages: rather than declaring all links, a node declares only the set of links with its neighbors that are its "*multipoint relays*". The use of *MPRs* also minimizes flooding of control traffic. Indeed only *multipoint relays* of one node forward control messages coming from this node. This technique significantly reduces the number of retransmissions of broadcast control messages [6, 9]. The two main OLSR functionalities, Neighbor Sensing and Topology Discovery, are now detailed.

3.1.1 Neighbor Sensing

Each node must detect the neighbor nodes with which it has a direct link. For this, each node periodically broadcasts *Hello* messages, containing the list of neighbors known to the node and their link status. The link status can be either *symmetric* (if communication is possible in both directions), *asymmetric* (if communication is only possible in one direction), *multipoint relay* (if the link is symmetric and the sender of the *Hello* message has selected this node as a *multipoint relay*), or *lost* (if the link has been lost). The *Hello* messages are received by all one-hop neighbors, but are not forwarded. They are broadcast once per refreshing period "*Hello_interval*" (the default value is 2 seconds). Thus, *Hello* messages enable each node to discover its one-hop neighbors, as well as its two-hop neighbors. This neighborhood and two-hop neighborhood information has an associated holding time, "*Neighbor_hold_time*", after which it is no longer valid. The default value is $3 * Hello\_interval$.

On the basis of this information, each node independently selects its own set of *multipoint relays* among its one-hop neighbors in such a way that the *multipoint relays* cover (in terms of radio range) all two-hop neighbors (see [9] for an algorithm example). Figure 1 illustrates the multipoint relays of a node m. The *multipoint relay* set is computed whenever a change in the one-hop or two-hop neighborhood is detected. In addition, each node m maintains its "*MPR selector set*". This set contains the nodes which have selected m as a *multipoint relay*. Node m only forwards broadcast messages received from one of its *MPR selectors*.

3.1.2 Topology Discovery

Each node of the network maintains topological information about the network obtained by means of *TC (Topology control)* messages. Each node m selected as a *multipoint relay*, broadcasts a *TC* message at least every "*TC_interval*" (the default value is 5 seconds). The *TC* message originated from node m declares the *MPR selectors* of m. If a change occurs in the *MPR selector* set, the next *TC* can be sent earlier. The *TC* messages are flooded to all nodes in the network and take advantage of *MPRs* to reduce the number of retransmissions. Thus, a node is reachable either directly or via its *MPRs*. This topological information collected in each node has also an associated holding time "*Top_hold_time*", after which it is no longer valid.

The neighbor information and the topology information are refreshed periodically, and they enable each node to compute the routes to all known destinations. These routes are computed with Dijkstra's shortest

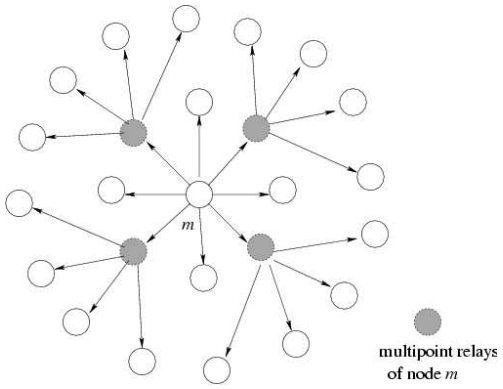

Figure 1: **Multipoint relays of node m.**

path algorithm [1]. Hence, they are optimal as concerns the number of hops. The routing table is computed whenever there is a change in neighborhood or topology information. In the next Section, we will see how the OLSR protocol behaves in real situations.

3.2 Platform Description

CELAR (French MoD / DGA) works on the concept of ad-hoc networks. These studies interest military programs like "Soldier of the Future", and could be fully integrated in RHD project (High Data Bit Rate Radio), for Navy and Land tactical networks. The objective of the MANET/OLSR CELAR tesbed is to evaluate and demonstrate the potential benefits of MANET advances in military tactical applications. As previously said, we focus more particularly on the following properties:

- auto-configuration,
- adaptability to topology changes,
- performances offered to user traffics,
- mobility support.

The CELAR MANET/OLSR platform, illustrated in Figure 2, is an actual network using 802.11b radio technology (WiFi) consisting of 18 MANET/OLSR nodes (10 routers, 4 VAIO laptops, 4 iPAQ PDAs). These nodes implement OLSR routing protocol (version 7, see [7]). This wireless network allows the communications between:

- the different floors of a building including a central tower (see routers R02 to R08 on figure 2);
- a shelter (see router R09 on figure 2);
- pedestrians with laptops or PDAs moving outside;
- and vehicles (see embedded routers R01 and R10 on figure 2).

This platform has been built at the end of December 2002 and is kept operational since. The MANET/OLSR platform includes the hardware listed in Table 1 and the software listed in Table 2. The wireless radio interfaces used are standard 802.11b interfaces. The technical specifications of the cards are given in Table 3.

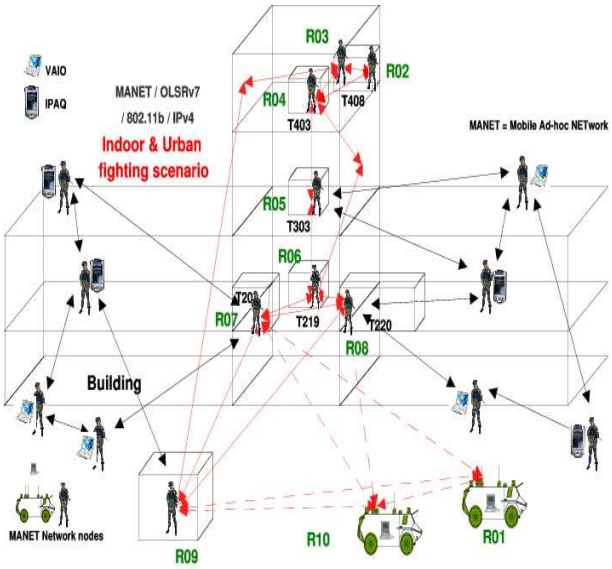

Figure 2: CELAR MANET/OLSR platform.

Equipment	Number	Type	Linux Distribution
OLSR Router	10	shipped by INRIA	shipped by INRIA
PDA	4	iPAQ ARM	Familiar
Laptop	4	Sony Vaio	Debian 3.0

Table 1: **Hardware of MANET/OLSR platform.**

Software	Description	Equipment
OLSR daemon	OLSR protocol version 7	PDA, Laptop, OLSR Router
iperf netperf	network performance tools	Laptop, OLSR Router
Misc.	monitoring software	Laptop

Table 2: **Software of MANET/OLSR platform.**

The OLSR implementation of the platform uses a power control mechanism, based on received power measurements, which is the one also experimented in [10]:

- Before a link to another node is accepted, the receive power of the corresponding *Hello*, must be above a threshold, which is set to *-85 dBm* in our experiments.
- As long as it is above a (lower) threshold, here equal to *-94 dBm*, and it is correctly refreshed, the link is considered valid.

Measures obtained with this MANET/OLSR platform are reported in Section 4.

Wireless device	PCMCIA, Avaya Wireless PC Card (Silver) (previously sold as “Orinoco Silver” and “Lucent Technologies Silver”)
Compatibility	IEEE 802.11b Standard for Wireless LANs (DSSS)
Firmware	tested with versions 6.04 and 7.52
MAC	CSMA/CA
R-F Frequency Band	2.4 GHz (2400-2500 MHz)
Used sub-channel	channel 11 (2462 MHz)
Modulation technique	Direct Sequence Spread Spectrum CCK (11 and 5.5 Mbps), DQPSK (1 Mbps), DBPSK (1 Mbps)
Spreading	11-chip Barker Sequence
Bit Error Rate	Better than 10^{-5}
Nominal Output Power	10 dBm

Table 3: **Radio specifications of MANET/OLSR platform, according to hardware documentation**

4 Measurements of OLSR Performance

4.1 OLSR Auto-configuration

In these first experiments, our goal is to show that (i) OLSR finds the shortest route to any destination and (ii) OLSR considers only links with acceptable quality. For that purpose, we measure for each router in the platform the following quantities representative of the OLSR router behavior:

- **the power of the received signal**: on a router, the power of the signal received from any other router allows to judge the signal quality over a radio link. This experiment is repeated at different times to study the power variations.
- **the shortest route to any destination**: the obtained values show that the shortest route to any destination reflect the fluctuations of the received radio signal.

The topology associated with these experiments is depicted in Figure 3. An additional link between R03 and R04 is present in some experiments (due to radio variability).

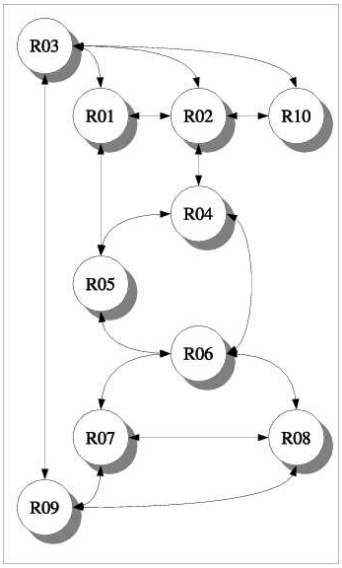

Figure 3: **Topology of the routers.**

4.1.1 Received power

In these experiments, we measure for each router the power of the radio signal received from any other router. For the platform, the power thresholds are respectively -85 dBm to accept and -94 dBm to reject a radio link. More precisely, in each experiment, we collect the average value of the received signal over a period of 10 seconds. The driver had been modified in order to get the power of the received signal: the reported value is given by the firmware of the wireless card. In this experiment, the received power is measured on the *Hello* messages, in the absence of user traffic. The experiment is repeated several times a day and on several consecutive days.

Table 4 and Table 5 report measures obtained the same day, but one minute later. On the other hand, Table 6 reports measures obtained the day after. Finally Table 7 gives the mean and the standard deviation obtained through all these experiments.

→	R01	R02	R03	R04	R05	R06	R07	R08	R09	R10
R01	-	-52	-40	-82	-88	.	.	.	.	-46
R02	-52	-	-59	-81	.	.	.	.	.	-66
R03	-48	-63	-	-82	-90	.	.	.	-79	-43
R04	-80	-80	-82	-	-50	-72	.	.	.	-86
R05	-85	.	-92	-48	-	-63	-89	-87	.	-93
R06	.	.	-92	-72	-59	-	-75	-76	.	.
R07	.	.	.	.	-91	-74	-	-59	-80	.
R08	.	.	.	.	-92	-76	-62	-	-82	.
R09	.	.	-80	.	.	.	-80	-83	-	.
R10	-48	-64	-43	-87	.	.	.	.	.	-

Table 4: **Received power: Experiment 1.**

→	R01	R02	R03	R04	R05	R06	R07	R08	R09	R10
R01	-	-52	-43	-82	-85	.	.	.	.	-43
R02	-53	-	-58	-80	.	.	.	.	.	-66
R03	-43	-62	-	-88	-89	.	.	.	-79	-49
R04	-81	-78	-87	-	-50	-72	.	.	.	-84
R05	-87	.	-91	-48	-	-65	-88	-87	.	.
R06	.	.	-91	-72	-58	-	-75	-76	.	.
R07	.	.	.	.	-90	-75	-	-59	-81	.
R08	.	.	.	.	-90	-77	-62	-	-82	.
R09	.	.	-79	.	.	.	-79	-82	-	.
R10	-45	-65	-45	-86	.	.	.	.	.	-

Table 5: **Received power: Experiment 2, one minute later.**

→	R01	R02	R03	R04	R05	R06	R07	R08	R09	R10
R01	-	-52	-48	-84	-85	.	.	.	.	-35
R02	-51	-	-58	-79	.	.	.	.	.	-52
R03	-49	-60	-	-88	.	.	.	.	-79	-47
R04	-89	-79	-87	-	-51	-71	.	.	.	-77
R05	-84	.	-91	-48	-	-64	-89	-84	.	-91
R06	.	.	-91	-73	-59	-	-73	-79	.	.
R07	.	.	.	.	-88	-74	-	-63	-81	.
R08	.	.	.	.	-87	-77	-65	-	-82	.
R09	.	.	-79	.	.	.	-80	-83	-	.
R10	-41	-59	-53	-82	.	.	.	.	.	-

Table 6: **Received power: Experiment 4, the day after.**

It can be noticed that the measures reported in Table 4 to 6 are **not symmetric**, naturally, sometimes noticeably so. For example, on Table 4, the power with which R06 received the radio signal from R05 is not equal to the power with which R05 received R06, as there is a $4dBm$ difference (this is confirmed in the table 7, with averages) ; $4dBm$ is the typical gain of small omnidirectionnal 802.11 antenna, so it is noticeable. Moreover, in the three tables, R03 receives the signal from R06 but the reverse is never true. This experiment gives an insight about to the **existence of asymmetric radio links** in the real world. Concerning the radio link quality, it ranges from -93 dBm, value obtained for instance on Table 4 by the link R05 → R10, to -35 dBm, value obtained for instance in Table 6 by the link R01 → R10. The radio link quality depends not only on the considered link but also at the day time. The same experiment repeated one minute later leads to different results, as observed in Table 4 and Table 5. These measures reflect the **time varying quality of radio links**. Moreover, some radio links are versatile. For instance, the link R05 → R10 exists on Table 4 and the day after (see Table 6), but not one minute later as shown in Table 5. This can be explained by the rejection threshold of -94 dBm.

Table 7 summarizes all the measures given in this subsection, by giving for each router the mean and the standard deviation of the power of the received radio signal from any other router. On the static network on which measurements were made, we can conclude that **the variations of the received powers are generally slight**, the standard deviation remaining generally below 3. There is an exception with router R10 where the standard deviation reaches 6 (e.g. routers R01 and R02 receiving from R10).

→	R01	R02	R03	R04	R05	R06	R07	R08	R09	R10
R01	-	-52.6 (2.2)	-44.5 (4.5)	-83.3 (2.4)	-87.6 (2.9)	- -	- -	- -	- -	-40.2 (6.1)
R02	-52.6 (1.8)	- -	-59.2 (2.7)	-80.1 (1.9)	- -	- -	- -	- -	- -	-56.6 (6.0)
R03	-45.2 (2.6)	-62.5 (2.8)	- -	-85.1 (2.4)	-90.8 (2.2)	- -	- -	- -	-80.2 (1.3)	-45.2 (3.9)
R04	-83.8 (3.7)	-79.7 (2.6)	-84.6 (2.3)	- -	-49.9 (0.8)	-71.6 (1.1)	- -	- -	- -	-82.3 (4.6)
R05	-86.8 (1.9)	- -	-90.8 (1.1)	-48.1 (0.8)	- -	-63.6 (0.8)	-89.3 (2.9)	-86.2 (1.4)	- -	-90.9 (3.6)
R06	- -	- -	-91.6/- (1.7)	-72.0 (1.0)	-59.0 (0.8)	- -	-73.7 (1.5)	-76.7 (1.8)	- -	- -
R07	- -	- -	- -	- -	-89.1 (1.5)	-74.7 (1.3)	- -	-60.8 (1.6)	-80.2 (1.0)	- -
R08	- -	- -	- -	- -	-89.7 (2.4)	-77.6 (1.5)	-63.2 (1.3)	- -	-81.8 (1.0)	- -
R09	- -	- -	-79.7 (0.9)	- -	- -	- -	-79.6 (0.8)	-82.5 (0.8)	- -	- -
R10	-45.3 (4.0)	-62.2 (2.5)	-46.5 (3.8)	-86.7 (3.3)	- -	- -	- -	- -	- -	- -

Table 7: **Average signal received (mean and standard deviation)**

4.1.2 Routes

Table 8, Table 9 and Table 10 show the path from any router to any other destination router corresponding to the same experiments as respectively Table 4, Table 5 and Table 6. This path is represented by the sequence of routers successively visited. It has been built from the routing tables present in each router. If in this table, two routers are separated by '/', it means that there is a temporary distance inconsistency in the routing tables due to the fact that some nodes have already updated their table while other ones have not yet. From the values reported in the tables, we can conclude that **there is no loop in OLSR routing** in this instance.

→	R01	R02	R03	R04	R05	R06	R07	R08	R09	R10
R01	-	1 2	1 3	1 4	1 4 5	1 4 6	1 3 9 7	1 3 9 8	1 3 9	1 10
R02	2 1	-	2 3	2 4	2 4 5	2 4 6	2 3 9 7	2 3 9 8	2 3 9	2 10
R03	3 1	3 2	-	3 4	3 4 5	3 4 6	3 9 7	3 9 8	3 9	3 10
R04	4 1	4 2	4 3	-	4 5	4 6	4 6 7	4 6 8	4 3 9	4 3 10
R05	5 4 1	5 4 2	5 4 3	5 4	-	5 6	5 6 7	5 6 8	5 4 3 9	5 4 3 10
R06	6 4 1	6 4 2	6 4 3	6 4	6 5	-	6 7	6 8	6 7 9	6 4 3 10
R07	7 6 4 1	7 6 4 2	7 9 3	7 6 4	7 6/2 5/0	7 6	-	7 8	7 9	7 9 3 10
R08	8 6 4 1	8 6 4 2	8 9 3	8 6 4	8 6/2 5/0	8 6	8 7	-	8 9	8 9 3 10
R09	9 3/2 1/0	9 3/2 2/0	9 3	9 3 4	9 3 4 5	9 7 6	9 7	9 8	-	9 3 10
R10	10 1	10 2	10 3	10 3/4 4/0	10 3 4 5	10 3 4 6	10 3 9 7	10 3 9 8	10 3 9	-

Table 8: **Routes: Experiment 1.**

→	R01	R02	R03	R04	R05	R06	R07	R08	R09	R10
R01	-	1 2	1 3	1 4	1 4 5	1 4 6	1 3 9 7	1 3 9 8	1 3 9	1 10
R02	2 1	-	2 3	2 4	2 4 5	2 4 6	2 3 9 7	2 3 9 8	2 3 9	2 10
R03	3 1	3 2	-	3 4	3 4 5	3 4 6	3 9 7	3 9 8	3 9	3 10
R04	4 1	4 2	4 3	-	4 5	4 6	4 6 7	4 6 8	4 3 9	4 10
R05	5 4 1	5 4 2	5 4 3	5 4	-	5 6	5 6 7	5 6 8	5 4 3 9	5 4/2 10/0
R06	6 4 1	6 4 2	6 4 3	6 4	6 5	-	6 7	6 8	6 7 9	6 4/2 10/0
R07	7 6 4 1	7 6 4 2	7 9 3	7 6 4	7 6/2 5/0	7 6	-	7 8	7 9	7 6 4/2 10/0
R08	8 6 4 1	8 6 4 2	8 9 3	8 6 4	8 6/2 5/0	8 6	8 7	-	8 9	8 6 4/2 10/0
R09	9 3/2 1/0	9 3/2 2/0	9 3	9 3 4	9 3 4 5	9 7 6	9 7	9 8	-	9 3/2 10/0
R10	10 1	10 2	10 3	10 4	10 4 5	10 4 6	10 3 9 7	10 3 9 8	10 3 9	-

Table 9: **Routes: Experiment 2, one minute later.**

→	R01	R02	R03	R04	R05	R06	R07	R08	R09	R10
R01	-	1 2	1 3	1 4	1 5	1 4 6	1 3 9 7	1 3/3 9/1 8	1 3 9	1 10
R02	2 1	-	2 3	2 4	2 1 5	2 4 6	2 3 9 7	2 3 9 8	2 3 9	2 10
R03	3 1	3 2	-	3 1 4	3 1 5	3 1 4 6	3 9 7	3 9 8	3 9	3 10
R04	4 1	4 2	4 1 3	-	4 5	4 6	4 6 7	4 6 8	4 1 3 9	4 10
R05	5 1	5 4 2	5 1 3	5 4	-	5 6	5 6 7	5 6 8	5 1 3 9	5 4 10
R06	6 4 1	6 4 2	6 4 1 3	6 4	6 5	-	6 7	6 8	6 7 9	6 4 10
R07	7 6 4 1	7 6 4 2	7 9 3	7 6 4	7 6 5	7 6	-	7 8	7 9	7 6 4 10
R08	8 6 4 1	8 6 4 2	8 9 3	8 6 4	8 6 5	8 6	8 7	-	8 9	8 6 4 10
R09	9 3 1	9 3 2	9 3	9 3 1 4	9 3 1 5	9 7 6	9 7	9 8	-	9 3 10
R10	10 1	10 2	10 3	10 4	10 1 5	10 4 6	10 3 9 7	10 3 9 8	10 3 9	-

Table 10: **Routes: Experiment 4, the day after.**

With these experiments, we can conclude that **routes provided by OLSR are the shortest ones as proved by the topology illustrated on figure 3 and are globally stable as shown by tables 8, 9 and 10**. The routing tables also illustrate how OLSR discovered the topology, and adapted to the disappeareance of the link between R03 and R04, present in table 8 and table 9, but not in table 10.

4.2 OLSR Adaptability

In this second series of experiments, we want to measure OLSR recovery time after a node appearance / disappearance. We proceed as follows: the OLSR daemon being running, we emulate node appearance/disappearance by changing back and forth the operational channel of the involved node. We experiment with $Vaio2$ switching back and forth between channel 11 and channel 1. The routes to $Vaio2$ are illustrated in figure 4.

We have checked that OLSR updates the routes according to the absence/presence of the considered node (here $Vaio2$) in order to maintain the shortest ones. Measured recovery times of OLSR daemon are given in Table 11. The resulting time precision is about 1 second (due to manual recording of times). In this table, the "off in sec value" (resp. "on in sec value") denotes the time after which the route to $Vaio2$ is no longer configured (resp. is configured) in the node designated by the table line, whereas the "mean" denotes the average value computed on the nodes being at the same hop number from $Vaio2$.

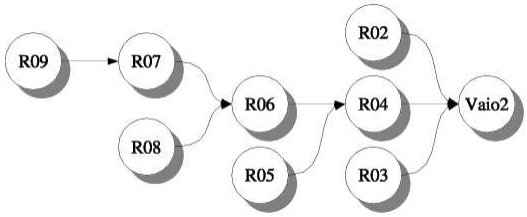

Figure 4: **The routes to** $Vaio2$

	hop number	off in sec		on in sec	
		value	mean	value	mean
R02	1	7.2 sec	6.7 sec	2.8 sec	2.8 sec
R03	1	7.0 sec		2.2 sec	
R04	1	5.8 sec		3.5 sec	
R05	2	7.0 sec	6.7 sec	4.8 sec	4.8 sec
R06	2	6.5 sec		4.8 sec	
R07	3	7.3 sec	7.3 sec	5.1 sec	5.1 sec
R08	3	7.3 sec		5.1 sec	
R09	4	7.1 sec	7.1 sec	5.7 sec	5.7 sec
All			7.0 sec		4.2 sec

Table 11: **Connection/Deconnection of** $Vaio2$

As we see, the results are consistent with OLSR timers suggested in the RFC 3626:

- The neighbor nodes of the appearing node, ($R02$, $R03$ and also $R04$ for $Vaio2$), need 0 to 4 seconds (0 to $2 * Hello\_Interval$) with a theoretical average of 2 seconds, for recognizing a neighbor.
- The neighbor nodes of the disappearing node, need 4 to 6 seconds, for considering the neighbor lost. The implementation needs a bit more, probably because of a coarse grained timer. In OLSR, a neighbor link disappears from the neighbor table in three possible cases:
  1. it has not been refreshed during $3 * Hello\_Interval$;
  2. the received signal power falls under the reject threshold;
  3. OLSR receives a link layer notification in case of a failed data transfer.

  In our experiment, because of the node disappearance emulation by channel switching, the second case is not possible. Moreover, our implementation OLSR doesn't receive link layer notification, excluding the third case. As a consequence, the only possible case is the first one. It should be noticed that the obtained values would have been shorter in the second and third cases.
- An appearing node, more than 2 hops away, appears in routing table after about 4 seconds (minimum 2 seconds, maximum 10 seconds). This time corresponds to the time needed to recognize a neighbor plus the time needed to propagate the topology change message advertising this new node.
- A disappearing node, more than 2 hops away, disappears in routing table after about 7 seconds (minimum 4 seconds, maximum 11 seconds). This time corresponds to the time needed to recognize the lost link plus the time needed to propagate the topology change message.

These results, obtained by measurement, are compatible with those given in [11], obtained by simulation for a MANET of 50 nodes.

4.3 Performances Offered to User Traffic

We now focus on the throughput offered to user traffic. The topology is the one depicted in Figure 3. We consider TCP flows and measure the throughput offered to each user flow on each node in the network. The experiment duration is 10 seconds. This duration is long enough for obtaining reproducible results. The available throughput is measured with Netperf. To ease the results interpretation, the throughput of each TCP flow is measured in the absence of any other user traffic.

Tables 12 to 14 summarize the results obtained with TCP. Like the received power tables, the throughput tables are not symmetric. For instance, the TCP flow $R02 \rightarrow R05$ receives a throughput of only 0.52 Mbps, while the TCP flow $R05 \rightarrow R02$ receives 1.55 Mbps (see Table 14). The values range from 0.16 Mbps (see in Table 14 the TCP flow $R07 \rightarrow R02$) obtained by nodes four-hop away to 5.14 Mbps (see in Table 14 the TCP flow $R06 \rightarrow R05$) obtained by nodes one-hop away. These tables show that generally the smaller the hop count between two nodes, the higher the available throughput between them. Exceptions exist: for instance in Table 13, the TCP flow $R02 \rightarrow R05$ between nodes two-hop away receives a smaller bandwith (0.54 Mbps) than the TCP flow $R03 \rightarrow R06$ between nodes three-hop away (1.51 Mbps).

→	R02	R03	R04	R05	R06	R07	R08	R09
R02	-	4.45	3.80	0.50	0.51	0.37	0.40	0.31
R03	4.76	-	2.94	1.74	1.69	0.74	0.91	5.03
R04	2.97	4.38	-	5.14	5.03	???	1.26	1.39
R05	1.59	1.99	5.10	-	5.09	2.59	2.15	1.21
R06	1.45	1.86	5.06	5.11	-	5.10	5.06	1.12
R07	0.39	0.60	0.66	2.25	5.09	-	3.08	???
R08	0.49	0.64	0.30	1.94	3.00	3.70	-	2.84
R09	0.51	4.99	1.64	0.65	0.55	2.97	2.59	-

Table 12: **Throughput in Mbps: Experiment 1**

→	R02	R03	R04	R05	R06	R07	R08	R09
R02	-	4.32	3.02	0.54	0.52	0.44	0.54	???
R03	4.81	-	2.80	1.54	1.51	0.79	0.59	4.99
R04	3.06	2.89	-	5.14	5.06	0.60	???	1.02
R05	1.67	1.82	5.09	-	5.12	2.60	2.41	0.96
R06	1.51	1.73	5.09	5.13	-	5.09	4.85	1.38
R07	0.47	0.45	0.63	2.59	5.06	-	3.37	2.91
R08	0.38	???	0.51	1.84	3.03	4.80	-	2.94
R09	0.70	4.97	1.47	0.59	0.64	2.93	2.20	-

Table 13: **Throughput in Mbps: Experiment 2**

→	R02	R03	R04	R05	R06	R07	R08	R09
R02	-	3.27	3.06	0.52	0.53	0.42	0.38	1.08
R03	4.62	-	3.00	1.85	1.84	0.50	0.51	5.01
R04	3.00	4.72	-	5.06	5.08	0.89	1.54	1.34
R05	1.55	1.73	5.09	-	5.09	1.31	1.94	1.26
R06	1.41	1.80	4.98	5.14	-	5.11	4.71	0.82
R07	0.16	0.34	0.62	2.61	4.86	-	3.89	3.36
R08	0.57	0.75	1.79	1.94	3.00	4.53	-	2.90
R09	0.41	4.97	1.21	0.58	0.52	4.34	2.24	-

Table 14: **Throughput in Mbps: Experiment 3**

Let us focus on Table 14 and consider three cases more carefully:

- If we first consider two nodes that are one-hop away, the throughput between them is generally high (i.e. 5.01 Mbps for R03 → R09 and 4.97 Mbps for R09 → R03). We now focus on the particular case of nodes R03 and R09, these two nodes are physically very far away in the platform (not in the sense of hop count: they are neighbors), however we measure high throughput between them. Notice that according to Table 4 R09 receives R03 at -79 dBm and R03 receives R09 at -80 dBm. Such a quality of radio link does not prevent high throughput. We can also conclude that the choice of power thresholds is good (-85dBm for the acceptance and -94 dBm for the rejection).

- The throughput between two nodes can unfrequently be the same in both directions. Consider for instance nodes R05 and R08 that are two-hop away, each of them uses router R06 to reach the other one. The throughput between them is equal in both directions (1.94 Mbps in Table 12 and 1.84 Mbps in Table 14).
- Finally, we consider nodes that are three-hop away like routers R02 and R07. The route from R02 to R07 is equal to R02 R03 R09 and R07, while the route from R07 to R02 is equal to R07 R06 R04 and R02. The throughput R07 $\rightarrow$ R02 is equal to 0.16 Mbps while it is equal to 0.42 for R02 $\rightarrow$ R07. This can be explained by the fact that both routes do not visit the same intermediate nodes (i.e. routers R03 and R09 for R02 $\rightarrow$ R07 vs routers R06 and R04 for R07 $\rightarrow$ R02).

As suggested by these experiments results, we now evaluate the influence of two factors on the available throughput: the received signal power and the hop number.

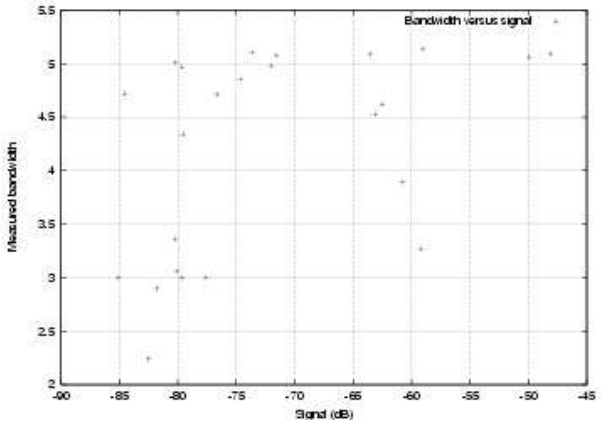

Figure 5: **Throughput versus received signal power**

Figure 5 represents the TCP throughput measured on a direct link: the duration was 10 seconds. For a good signal (i.e. -60 dBm), the throughput is generally higher than 5 Mbps. However, for such a signal, there exist routers for which the throughput is weak (i.e. around 3.2 Mbps). This can be explained by the multipath phenomenon. On the other hand, when the signal quality is weak (i.e. -85 dBm), we can also obtain high throughput (i.e. around 5 Mbps), but less frequently. Figure 5 shows that for a signal received with a power higher than -85dBm, the measured throughput can reach the highest possible value. As a consequence, these measures allow **to justify the choice of the power thresholds we have made**. Moreover, these thresholds are very close to the ones provided by the IEEE 802.11 card constructors.

Figure 6 investigates the available throughput with respect to the number of hops. We observe three clouds of points: the first one corresponds to a distance of 1 hop, the second one corresponds to a distance of 2 hops and the last one corresponds to 3 hops. The available throughput measured between two nodes generally decreases with the number of hops. **These results are corroborated by simulation results made with NS2** as shown by Table 15. In the simulations, we assume an interference radius equal to two times the coverage radius, the TCP packet size is 1500 bytes. The measured average is obtained by averaging the bandwidth values measured during experiments 1, 2 and 3, after having discarded values corresponding to routes having links with a small bandwidth, like $R02 \leftrightarrow R04$, $R08 \rightarrow R06$, $R08 \leftrightarrow R09$ and $R09 \leftrightarrow R07$.

In conclusion, the throughput available between two nodes depends both on the number of hops between them and on the received signal power. Notice that power thresholds play their role by rejecting links of bad quality.

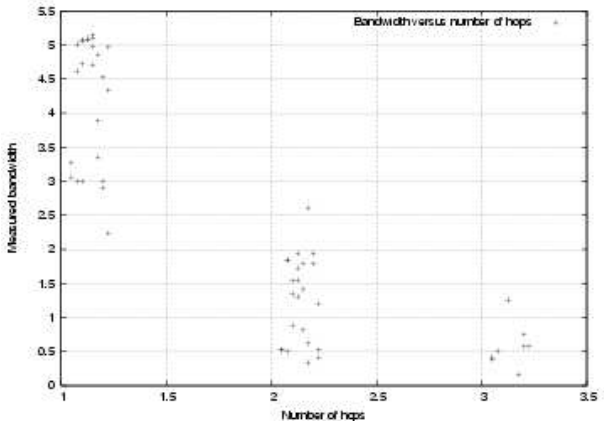

Figure 6: **Throughput versus number of hops**

Hop number	Simulation	Measured average
1	4.6 Mbps	4.35 Mbps
2	2.34 Mbps	2.17 Mbps
3	1.59 Mbps	1.51 Mbps

Table 15: **Comparison with simulation results.**

We now study the influence of the RTS/CTS option. This option has been introduced to solve the hidden node problem. When the RTS/CTS option is used, the transmission of any message whose size is higher than a minimum size (8 bytes in our experiments) is preceded by the exchange of a Request To Send frame (RTS) followed by a Clear to Send (CTS) one. For the experiment whose results are given in Table 16, the option RTS/CTS has been switched on. **Globally, the throughput obtained with RTS/CTS is significatively smaller than this obtained without RTS/CTS, as in our experiments the overhead (i.e. additional delay) introduced by RTS/CTS fails to be compensated by some benefits.** For instance, the highest throughput, obtained on the link r6 $\rightarrow$ R05, is 3.78 Mbps instead of 5.14 Mbps.

$\rightarrow$	R02	R03	R04	R05	R06	R07	R08	R09
R02	-	3.53	2.39	0.51	0.56	0.34	0.41	1.51
R03	3.73	-	2.47	1.62	1.48	0.61	0.67	3.68
R04	2.35	2.58	-	3.78	3.67	0.81	1.54	???
R05	1.21	1.43	3.77	-	3.76	1.88	1.87	0.78
R06	1.20	1.35	3.76	3.78	-	3.76	3.50	1.08
R07	0.43	0.50	0.61	1.88	3.73	-	3.74	3.15
R08	0.49	0.69	1.19	1.53	2.51	3.74	-	2.87
R09	0.15	3.69	0.87	0.48	0.56	3.30	2.39	-

Table 16: **Throughput in Mbps: Experiment 4 with RTS/CTS**

It is naturally expected that in some cases, RTS/CTS will decrease the performance (since this adds extra exchanges and delays in the 802.11 MAC protocol, each node needs to send a 'Ready To Send' packet and has to wait for a 'Clear To Send' answer before transmitting its packet). However the aim and the expectation are that performance would be improved in some cases by alleviating the "hidden node" problem.

4.4 Mobility Support

We consider two scenarios representative of different mobility types:

- in the pedestrian scenario, a mobile node $M1$ moves at pedestrian speed inside the central tower hosting the platform, while the other nodes are immobile inside the tower or the shelter.
- in the vehicle scenario, one Vaio is embedded in a vehicle moving around the central tower.

4.4.1 Pedestrian mobility

In this subsection, the mobile node is an additional router called $M1$. The topology of the routers is illustrated in Figure 3. The routers are immobile inside the building, hosting the platform. Mobile node $M1$, while it is moving, sends a TCP flow to router R03. The trajectory of mobile node $M1$ is as follows, $M1$ starts from point called $T408$ located at level 4 on the platform. It goes to point $T403$ always at level 4. It then arrives in front of the stairs, point denoted $\rightarrow E1$, goes downstairs. It then arrives at level 3, point denoted $E1 \rightarrow$. It then moves to the point $T303$. It then arrives in front of the stairs, point denoted $\rightarrow E2$. It goes downstairs, arrives at level 2, walks until point $T220$. It then takes the lift upstairs, visiting successively levels 2, 3 and 4. At level 4, it comes back to point $T403$ and finally stops at point $T408$.

Figure 7 shows how the throughput available on the mobile node $M1$ varies while this router is moving. As we are interested in the possible connectivity loss, we focus on Figure 8 using a logarithmic scale on the y-axis. We observe three phases:

- at a time $t < 220$, the obtained throughput is at its maximum;
- for time t such that $220 \leq t \leq 560$, the throughput decreases. It becomes quasi-null in the time intervals 230-280, 325-340, 430-450 and 540-550, where the connectivity is lost: $M1$ has no neighbor. As soon the connectivity is obtained, TCP tries its best to progressively recover from packet or acknowledgement losses (progressive increase of the congestion window);
- for time $t > 560$, the obtained throughput is again at its maximum.

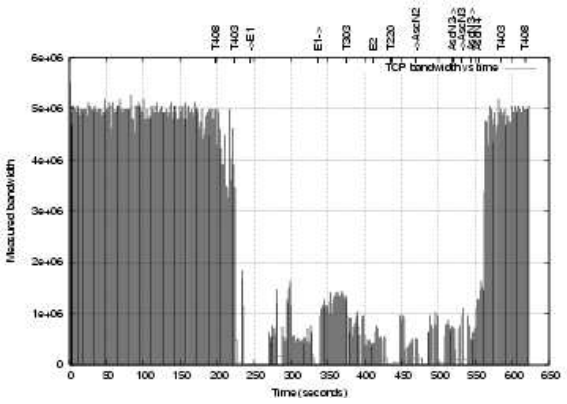

Figure 7: **TCP throughput vs time**

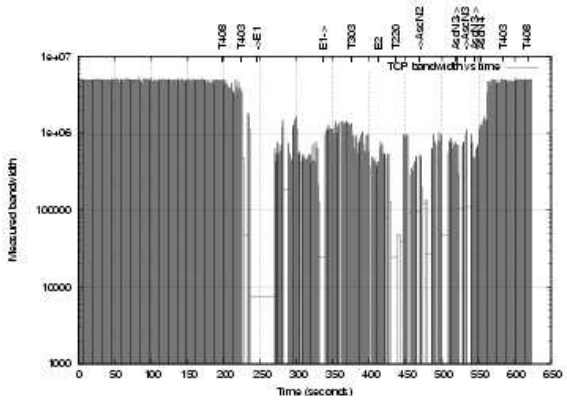

Figure 8: **TCP throughput vs time (log. scale on y axis)**

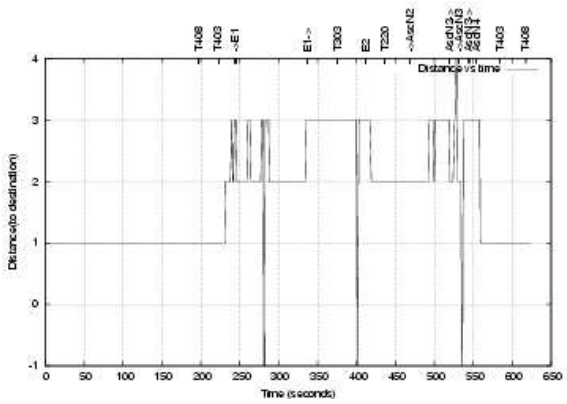

Figure 9: **Hop number to destination vs time.**

Figure 9 shows the variations of the distance to the destination router R03 while $M1$ is moving. On this figure, -1 on the y-axis means that there is no route to destination. This happens for example at times 280, 400 and 540. In these cases, the connectivity loss is explained by the absence of neighbor for $M1$, as shown by Figures 11 to 13. Figure 10 depicts the changes in the choice of the next hop to reach the destination router R03, while mobile node $M1$ is moving.

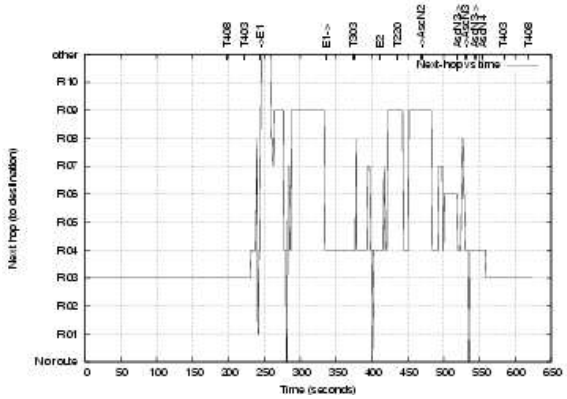

Figure 10: **Next hop to destination vs time.**

Figures 11 to 13 illustrate the variations of the received signal power while mobile node $M1$ is moving. As expected, the variations of the received power of radio signal are increased by mobility. For example, we can consider the three following cases:

- At a time $t < 240$, R03 is a neighbor of $M1$. Consequently R03 is the next hop. Figure 11 shows that $M1$ receives R03 with a power higher than the reject threshold (-94 dBm).
- For a time $330 < t < 380$, R04 is the next hop of $M1$ to reach R03. Indeed, during this time interval, as corroborated by Figure 12, $M1$ receives R04 with a power higher than the acceptance threshold (-84 dBm).
- Finally, for a time $420 < t < 480$, R09 is the next hop chosen by $M1$ to reach R03. Figure 13 shows that during this time interval, $M1$ receives R09 with a power higher than the acceptance threshold.

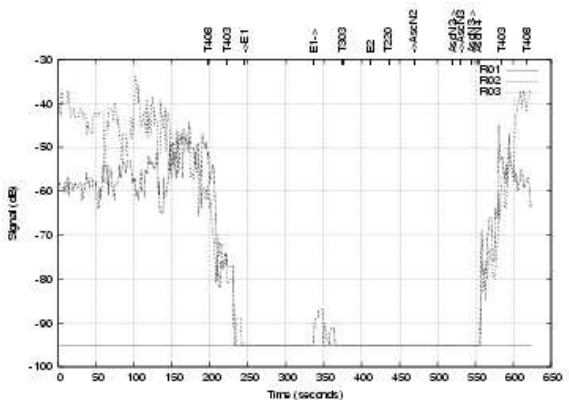

Figure 11: **Signal power received by $M1$ from R03 vs time.**

The power received from router R01 is under the power threshold. Hence there is no link R01 $\rightarrow M1$. Consequently $M1$ never choses R01 as the next hop to R03: this is corroborated by Figure 10.

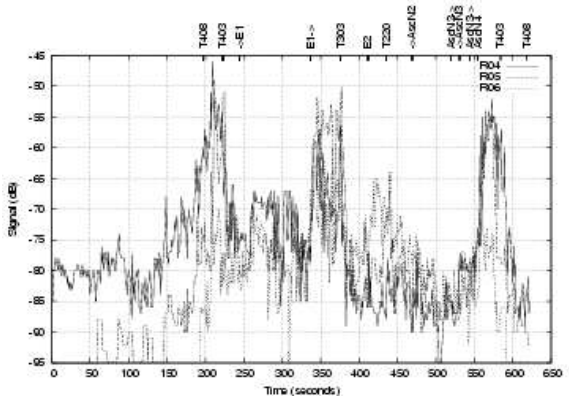

Figure 12: **Signal power received by $M1$ from R04 vs time.**

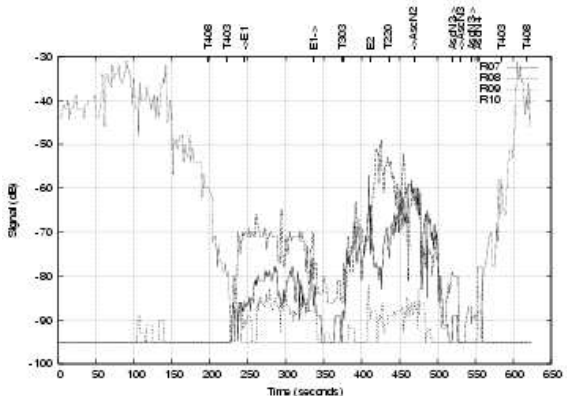

Figure 13: **Signal power received by $M1$ from R09 vs time.**

This experiment shows that:

- the power threshods are useful to detect mobility: the link is considered broken as soon as the received signal power falls under -94dBm, instead of waiting 6 seconds after the receipt of the last *Hello*;
- OLSR detects topology changes and updates routes accordingly, selecting a next hop received with an adequate power;
- the change of received power with mobility, even on some small time scale (like 10 seconds), is noticeable compared to the variation of power on a static network. For instance, the standard deviation of the signal power received from R04 by mobile node M1, computed on time intervals of 10 seconds, is 6.8, whereas it was less than 3 in the static case;
- it takes time to TCP to increase the congestion window to its maximum size. To focus on OLSR behavior and avoid this side-effect, we consider only UDP traffics in the following experiment.

4.4.2 Vehicle mobility

We now focus on a node (the laptop $Vaio3$ in our experiment) embedded in a vehicle moving around the building hosting the platform. Meanwhile, router R02 sends UDP traffic to $Vaio1$, $Vaio2$, and $Vaio3$ (one UDP flow at 16 kbps per destination). The topology of the network is illustrated in Figure 14. The routers are immobile inside the building, and other laptops ($Vaio1$ and $Vaio2$) are outdoor and do not move. The links with $Vaio3$ change depending on its position (this explains the dotted lines in Figure 14).

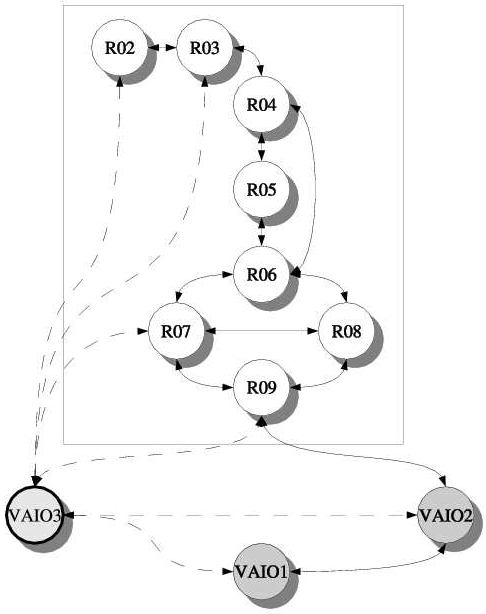

Figure 14: **Topology of the network during the mobility experiments.**

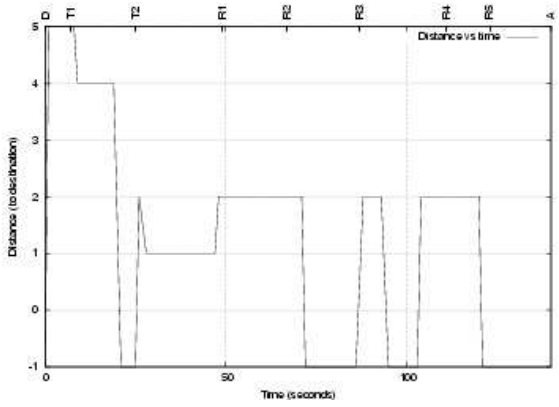

Figure 15: **Distance to router R02 vs time.**

We focus on $Vaio3$, the moving node. Figure 16 shows three time intervals with no route: $[21, 26)$, $[73, 86)$ and $[97, 103)$:

- In $[21, 26)$, the quality of the link with R07 decreases and Hellos are lost leading to a link breakage. At time $t = 22$, $Vaio3$ starts to receive R03 with a power higher than -85 dBm (see Figure 17). It then takes two Hello periods (i.e. 4 s) to establish a symmetric link. Notice that according to Figure 18, $Vaio3$ does not receive R06, R07, R08 or R09 after time 23. Moreover, Figure 19 shows that $Vaio3$ does not receive $Vaio1$ or $Vaio2$ before time 28. This explains why there is no route in $[21, 26)$;
- Before time $t = 73$, R03 was selected as the next hop. At time $t = 71$, there is a sudden decrease in the received signal power leading to a link breakage between $Vaio3$ and R03. When at time $t = 74$, the received power becomes higher than or equal to -85 dBm, it is not higher than -94 dBm for the duration needed to establish a symmetric link. Hence $Vaio3$ cannot use R03 as next hop. Finally, at time $t = 79$, R03 is again received with a power higher than -85 dBm and the received power stays

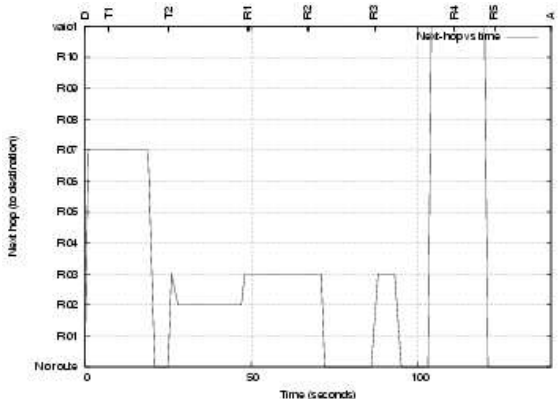

Figure 16: **Next hop to router R02 vs time.**

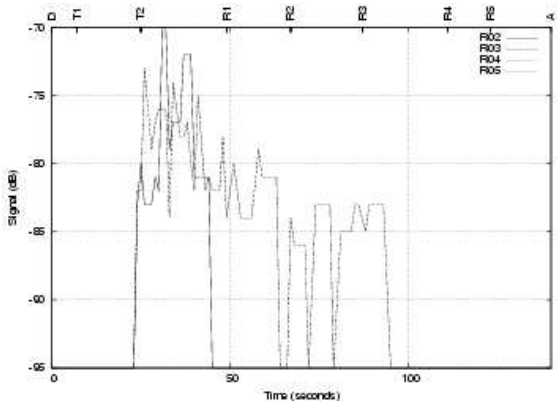

Figure 17: **Signal power received by $Vaio3$ vs time.**

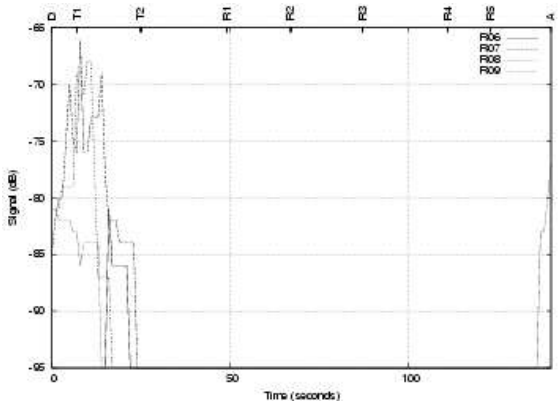

Figure 18: **Signal power received by $Vaio3$ vs time.**

over -94 dBm while more than 4 s (i.e. two Hellos periods) allowing to establish a symmetric link at time $t = 83$. This explains why there is no route in the time interval $[73, 86)$;

- Before time $t = 97$, $Vaio1$ was selected as the next hop. At time $t = 97$ there is a sudden decrease in the received signal power leading to a link breakage between $Vaio1$ and $Vaio3$. When at time $t = 99$, the received power becomes higher than or equal to -85 dBm, the symmetric link between $Vaio1$ and

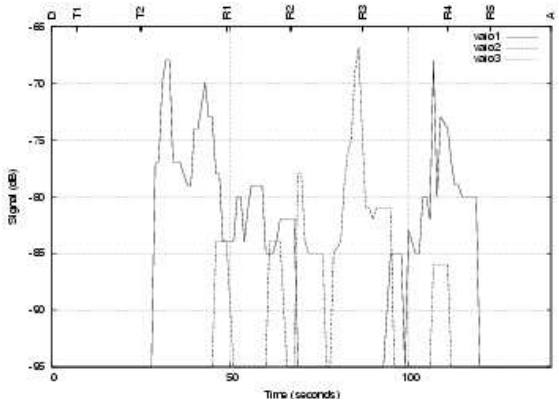

Figure 19: **Signal power received by $Vaio3$ vs time.**

$Vaio3$ is established at time $t = 103$. $Vaio3$ selects again $Vaio1$ as next hop. This explains the time interval $[97, 103)$, while there is no route.

This scenario is another illustration of the behavior of the OLSR protocol with mobility. OLSR performances in this scenario could be improved by giving OLSR messages a priority higher than this granted to user messages. in such a case, OLSR messages would be processed before user messages, allowing to update routes. Hence, user packets can use an updated route and reach their destination, instead of being lost on a no longer valid route.

5 Conclusion

Mobile ad-hoc networks are autonomous, self-adaptive and support mobility. These qualities make them essential for rescue applications, intelligent transportation systems and military tactical applications. To succeed, these networks must achieve good performance. That is the reason why we have built a MANET platform to quantitatively evaluate the behavior of such networks equipped with the OLSR routing protocol. As reported in this paper, the measured recovery times of OLSR after the appearance or disappearance of a link, router or terminal are consistent with OLSR timers as suggested in the RFC. The overall results show that the OLSR protocol and its implementation provide ad-hoc network connectivity and routing, with good performance. In scenarios with mobility, the adaptability of the OLSR protocol was evidenced, with appropriate changes of routes. The power measurements show that nevertheless with mobility, links can change greatly with time. This high variability of links and additionnally the delays introduced in the routing changes, show that some tuning of OLSR parameters (like message emission intervals) might improve the performance. This improvement has been introduced in OLSR version 11, the version corresponding to the RFC: the link refreshment period, $Hellointerval$, can be set per link. A shorter link refreshment period leads to an earlier detection of broken links and new links. Moreover, the overhead, directly related to the refreshment period, can be calibrated by the node velocity. In general, the measurements performed on this platform allow to conclude that OLSR routing seems to be well adapted to the applications considered e.g. (rescue, military tactical, intelligent transportation,...). Further work is needed to introduce quality of service in such networks and to allow service differentiation. Security and multicast traffics are further issues for MANETs in such a context.

References

[1] A. S. Tanenbaum, *Computer Networks*, Prentice Hall, 1996.

[2] C. Perkins, E. Belding-Royer, S. Das, *Ad hoc On-Demand Distance Vector (AODV) Routing*, IETF: The Internet Engineering Task Force, July 2003, RFC 3561.

[3] D. Johnson, D. Maltz, Y-C. Hu, *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*, IETF: The Internet Engineering Task Force, April 2003, draft-ietf-manet-dsr-09.txt, work in progress.

[4] J. Moy, *Open Shortest Path First (OSPF) Version 2*, IETF: The Internet Engineering Task Force, January 1998, RFC 2328.

[5] R. G. Ogier, F. L. Templin, M. Lewis, *Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)*, IETF: The Internet Engineering Task Force, RFC 3684, February 2004.

[6] P. Jacquet, P. Muhletaler, A. Qayyum, A. Laouiti, T. Clausen, L. Viennot, *Optimized Link State Routing Protocol*, IEEE INMIC, December 2001, Pakistan.

[7] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, *Optimized Link State Routing Protocol*, IETF: The Internet Engineering Task Force, November 2002, draft-ietf-manet-olsr-07.txt, work in progress.

[8] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, *Optimized Link State Routing Protocol*, IETF: The Internet Engineering Task Force, RFC 3626, October 2003.

[9] A. Qayyum, A. Laouiti, L. Viennot, *Multipoint relaying technique for flooding broadcast messages in mobile wireless networks*, HICSS: Hawai International Conference on System Sciences, January 2002, Hawai, USA.

[10] A. Laouiti and C. Adjih, *Mesures des performances du protocole OLSR*, IEEE SETIT 2003 Tunisia March 2003 (in French).

[11] A. Qayyum, *Analysis and evaluation of channel access schemes and routing protocols for wireless networks*, Phd Thesis, University of Paris Sud, November 2000.