INTERNSHIP REPORT

Contention-based waveform
for ad hoc tactical communications

THALES COMMUNICATIONS

Responsable de stage :
Marc Bieth

THALES Communications

160, Boulevard de Valmy
92 730 Colombes
France

Guillaume-Jean Herbiet

Ingénieur Supélec
Student in Master of Science in Computer Science,
Georgia Institute of Technology

ABSTRACT

The development of info-centered warfare along with available services through the IP-based protocols lead to a noticeable evolution of tactical communications as they now require a larger bandwidth and an increased flexibility (with self-configuring networks and information spread not anymore depending on the military hierarchy).

Thales Communication answers to these requirements by developing tactical nodes based on software defined radios (programmable devices where the waveform in use is not linked to the hardware) that are organized in mobile ad hoc networks (where connection and routing are automatically established regarding the current topology).

Several civilian solutions, based on the use of the IEEE 802.11 standard (Wi-Fi) in a multi-hop context with ad hoc routing protocols, such as OLSR, are currently developed and show a relatively different approach from the choices made by Thales.

Therefore, this study, after a presentation of the different technologies involved in those solutions, describes the design and implementation on the OMNET++ network simulator OLSR of a protocol stack model, based on CSMA/CA (medium access control of the IEEE 802.11 standard) and the OLSR routing protocol.

This model is then used to simulate the behaviour of a network of nodes using this stack so as to measure reachable performances under several topology and traffic scenarios.

This study reckons that, even if the contention-based protocol stack has acceptable behavior under given scenarios, it doesn't seem to be robust enough to be used under tactical constraints.

So as to address the weaknesses of the implemented solution, several improvements, based on more recent standards (such as IEEE 802.11e) or on ongoing researches (like OLSR protocol modifications) are suggested.

INDEX

1. CONTEXT OF STUDY 5
1.1 THALES COMMUNICATIONS 5
1.2 SOFTWARE DESIGNED RADIO DEPARTMENT 5
1.2.1 SOFTWARE DEFINED RADIO GOALS AND FEATURES 6
1.2.2 A FAVORABLE CONTEXT FOR THE DEVELOPMENT OF SOFTWARE RADIO 6
1.2.3 AN EXAMPLE OF APPLICATION: TACTICAL NETWORKS 7
1.3 THE AD-HOC NETWORK CONCEPT 7
1.3.1 MANET PARADIGM 7
1.3.2 INTEREST OF AD-HOC NETWORKS 8
2. OPTIMIZED LINK STATE PROTOCOL 9
2.1 OLSR PRINCIPLES 9
2.2 EXCHANGED MESSAGES 10
2.2.1 MULTIPLE INTERFACE DECLARATION (MID) 10
2.2.2 MESSAGES HELLO 10
2.2.3 MESSAGE TC (TOPOLOGY CONTROL) 11
2.2.4 HNA MESSAGE (HOST AND NETWORK ASSOCIATION) 11
2.3 OLSR IN A NUTSHELL 12
2.3.1 NEIGHBORHOOD DETECTION 12
2.3.2 MPR ELECTION 12
2.3.3 ROUTING TABLE COMPUTATION 13
3. SIMULATION FRAMEWORK 14
3.1 OMNET++ AND THE MOBILITY FRAMEWORK 14
3.2 SIMULATION DESIGN AND IMPLEMENTATION 14
3.2.1 TRAFFIC GENERATOR 16
3.2.2 MOBILITY MANAGEMENT 16
3.2.3 DATA ROUTING 16
3.2.4 CHANNEL ACCESS 16
3.2.5 RADIO CHANNEL MODELING 18
4. SIMULATION AND RESULTS ANALYSIS 19
4.1 AN OPERATIONAL SCENARIO: SECURING BRINON 19
4.1.1 SCENARIO DETAIL 19
4.1.2 RESULTS AND ANALYSIS 20
4.2 SYNTHESIS OF RESULTS 23
5. CONCLUSION 24

TABLE OF FIGURES

Figure 1.1 : Thales Communications at Colombes, France 5
Figure 1.2 : Software radio key features and related technical issues 6
Figure 1.3 : Info-centred warfare 7
Figure 2.1 : Optimized flooding with MPR 9
Figure 2.2 OLSR packet format 10
Figure 2.3 : MID message 10
Figure 2.4 : HELLO packet format 11
Figure 2.5 : TC packet format 11
Figure 2.6 : Network after MPR election by N0 13
Figure 3.1 : OMNeT++ simulation environment 14
Figure 3.2 : Simulation architecture 15
Figure 3.3 : Inter-frame spacing details 17
Figure 4.1 : Map of the simulated scenario 19
Figure 4.2 : Percentage of received packets for different flows 20
Figure 4.3 : Evolution of the MAC queue sized during simulation 21
Figure 4.4 : Evolution of the neighborhood of node 2 during the simulation 22

INDEX OF TABLES

Tableau 3.1 : Inter-frame spacings for the IEEE 802.11 standards and the tactical waveform 17
Tableau 4.1 : Simulation results for UDP traffic 20
Tableau 4.2 : Synthesis of performances and suggested improvements 23

CONTENTION-BASED WAVEFORM FOR AD HOC TACTICAL COMMUNICATIONS

1. CONTEXT OF STUDY

This part describes the context of my internship, including a brief presentation of Thales Communications and an introduction to the different technologies included in my work.

1.1 THALES COMMUNICATIONS

Thales is an internationally recognized company, designer and provider of electronic and communication systems for the military, national defense and security-related applications.

Implanted worldwide, Thales counts more than 60,000 collaborators in more than 50 countries and reached a sales amount of 10.3 milliards of Euros in 2005.

Figure 1.1 : Thales Communications at Colombes, France

Leader in aeronautics, defence and security, Thales provides its customer a constant innovation with an average 250 invention per year, validated by around 12 000 patents.

1.2 SOFTWARE DESIGNED RADIO DEPARTMENT

The recent decades have seen a large increase in the number of analog or digital communication standards being defined, both in the civil and military context. This multiplication of definitions makes even harder the task to establish common worldwide standards and future mobile systems, due to the competition between Asia, Europe and America, are likely to use different communication protocols.

On the other hand, today's wireless services are more and more ubiquitous and the global communication infrastructure requires them to be more flexible and reconfigurable so as to offer complements or at times completely substitute to wired communications, using the proliferation of services offered over satellites, cellular networks and other wireless WANs or LANs.

In the context of Thales activities, the Software Designed Radio department, is in charge of developing tactical communication nodes based on the software radio concept that allows to make the hardware and the waveform used for communications independent. This part describes some key features and benefits of the software radio concept along with an example of application in the field of tactical communications.

1.2.1 Software defined radio goals and features

In this context, the concept of software defined radio appears as a potential pragmatic solution so as to achieve interoperability between standards, while using a software implementation of the user terminal enabling a dynamic adaptation to the radio environment and standards in use at that time and for the current communications.

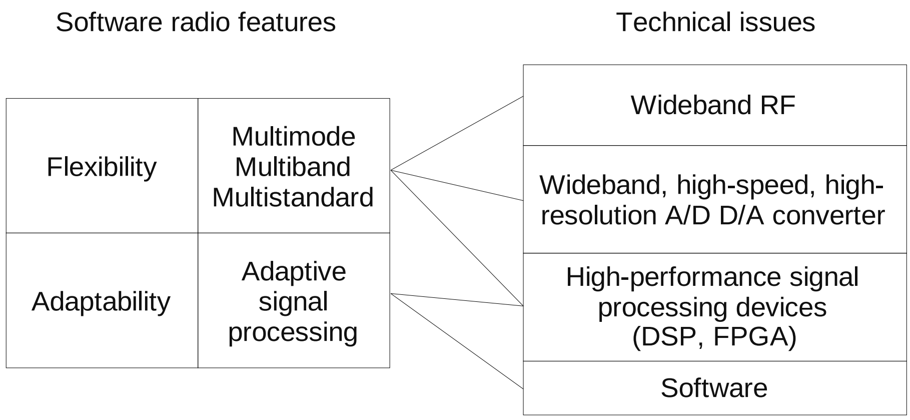

Software radio features
Technical issues
Flexibility
Multimode Multiband Multistandard
Adaptability
Adaptive signal processing
Wideband RF
Wideband, high-speed, high-resolution A/D D/A converter
High-performance signal processing devices (DSP, FPGA)
Software

Figure 1.2 : Software radio key features and related technical issues

Therefore, software radios implications are an increased ability to tolerate and support interoperability across heterogeneous air interface technologies, a better support for network upgrades and a substitution of general-purpose hardware to particular waveform-dedicated components. Besides, as those techniques improve the management of channel congestion and allow the use of a more flexible spectrum usage model.

1.2.2 A favorable context for the development of software radio

Moving to the concept of software radio allows an increased flexibility (in terms of customization, evolution and even a faster time-to-market) at lower costs . But other factors are pushing for software radios to be realized in commercial markets and are described in this paragraph.

Recent advances in hardware technology, smart antennas, adaptive power management and modulation and signal processing techniques make software designed radios feasible, despite the major design issues that remain (which are described further in this document). Those steps forward are welcome as an answer to the multiplicity of communication standards (due for example to different spectrum allocation in different countries).

These developments are ensured by commercial market opportunities. The military has been the first field of use for software radios but today the development of new wireless devices and the associated multimedia services providers to mix different media for delivering different types of service and create a new market for this concept.

1.2.3 An example of application: tactical networks

Software defined radio systems are reckoned as the key component for radio communication in the tactical domain of “network centric warfare”. The concept of software radio offers interoperability during joint and combined operations while unities may be using different radio systems from different suppliers, using new radio technologies or legacy systems with a frequency range from HF to UHF.

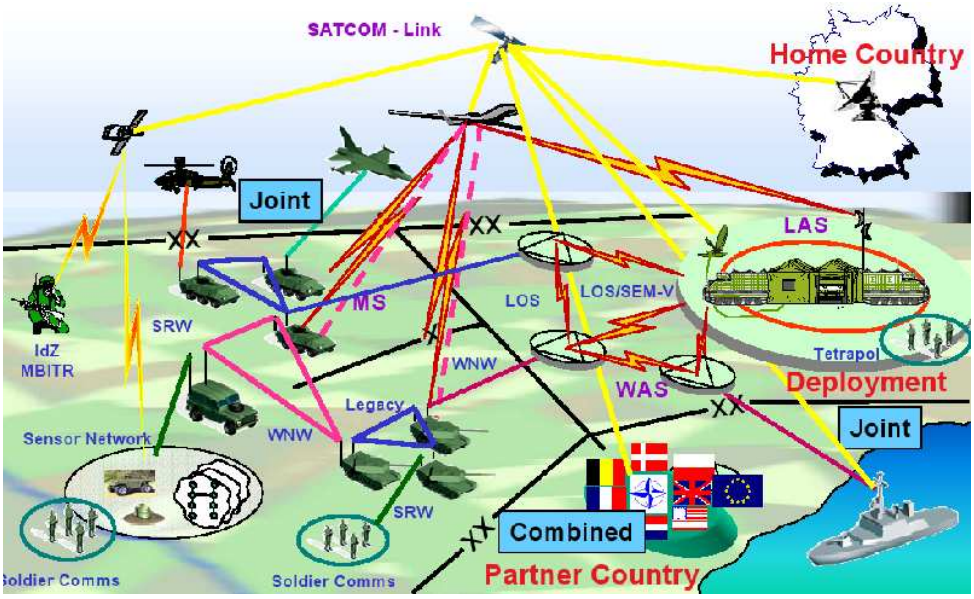


Figure 1.3 : Info-centred warfare

Besides, software designed radios allow support for high data transmission capabilities by using high data rate waveforms (WNW) and for integrated networking functions of the radio nodes that are key enabler to build tactical mobile ad-hoc radio networks (MANET).

1.3 The ad-hoc network concept

The developments of communication technologies in the military or civilian field lead to an explosion of the number of terminals and applications which can't rely on the traditional communication model, based on a static wired architecture and are the major reason for the current advances in wireless mobile ad-hoc networks (MANETs).

1.3.1 MANET paradigm

Wireless mobile ad-hoc networks are self-organized and self-configured allowing multi-hop communications between terminals through the air in a dynamically changing network.

A MANET network therefore allows mobile terminals to establish communications anytime and anywhere without any centralized infrastructure.

1.3.2 Interest of ad-hoc networks

Ad-hoc networks are really interesting when it comes to military tactical communications, but it can also play an important part in civilian applications like covering conventions or conferences, or enabling interactive computer-based classrooms.

Besides, they can be a concrete solution to restore communications in a crisis context where all other infrastructure collapsed, like after a natural disaster.

2. Optimized Link State Protocol

This part describes in further details one of the key technologies used in the development of the ad-hoc waveform proposed and assessed in this document. Those are the ad-hoc routing protocol (OLSR) and the IEEE 802.11 standard, used as reference for the channel access control mechanism and modified so as to be used in a tactical context.

OLSR is a proactive link-state routing protocol developed at INRIA. It uses periodic exchanges of messages so as to discover and spread data on network topology.

2.1 OLSR principles

OLSR tries to limit the amount of control messages by optimizing the number of broadcast transmissions required to flood the network. Therefore, each node elects Multipoint Relay Selectors (or MPR) which will be the only neighbors to retransmit its control packets.

In OLSR standard configuration, only MPR announce their links with their selectors which is sufficient to find a route from any node to any other node in the network.

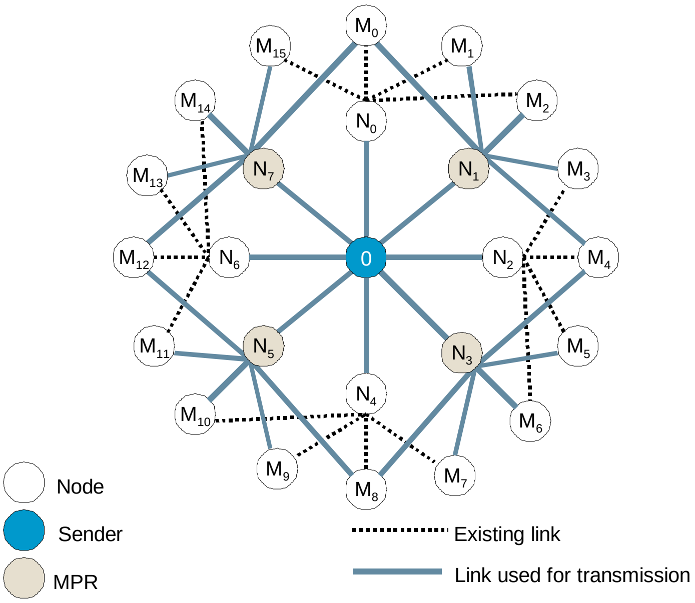


Figure 2.1 : Optimized flooding with MPR

OLSR exchanges control messages on UDP port 698, using a unified packet format which allow piggybacking of several messages and is compatible with both Ipv4 and IPv6.

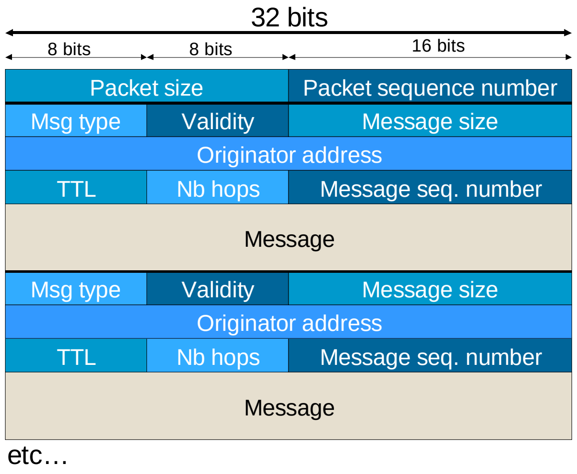


Figure 2.2 OLSR packet format

2.2 Exchanged messages

So as to discover and spread information on the network topology, OLSR uses four kind of control messages.

2.2.1 Multiple Interface Declaration (MID)

Each node with multiple interfaces periodically announces the list of addresses their interfaces and the address of the interface selected as "primary interface" which uniquely identifies the node on the network.

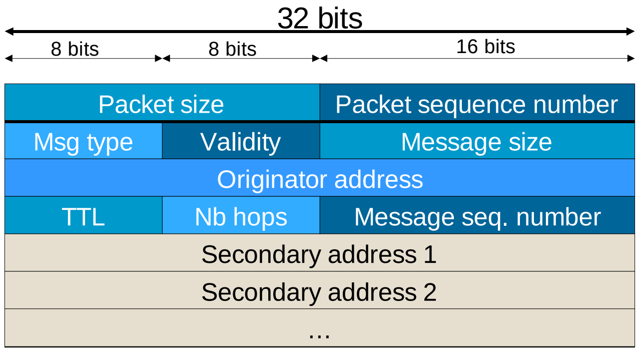
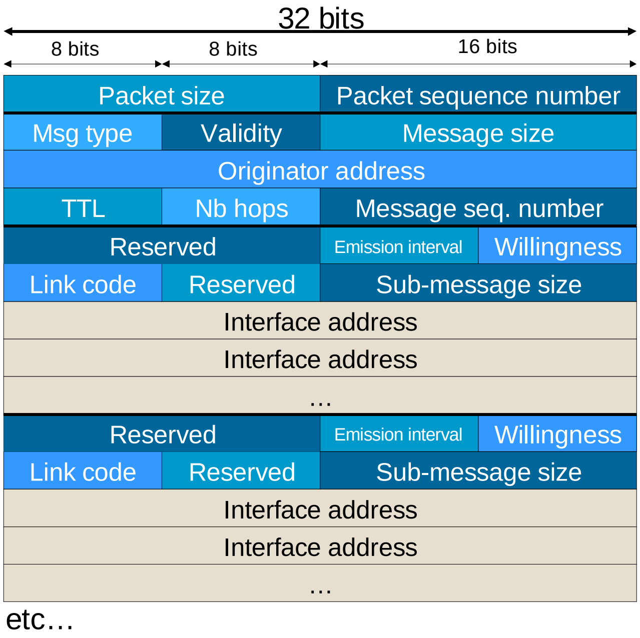


Figure 2.3 : MID message

2.2.2 Messages HELLO

This message is periodically exchanged only between neighbors and allow to perform topology discovery. It carries the list of neighbors with the state of the corresponding link (unspecified, lost, asymmetrical, symmetrical or link to an MPR) along with the willingness of this neighbor to route data.



32 bits

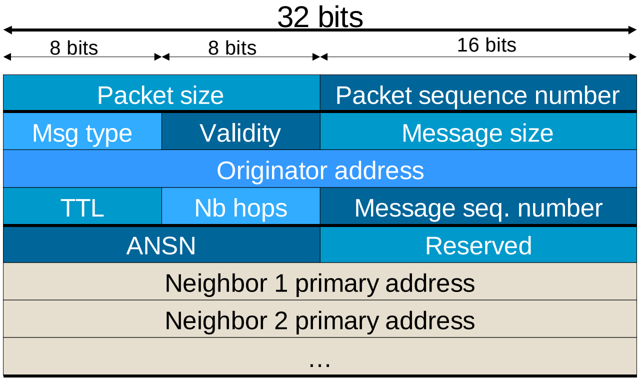
8 bits	8 bits	16 bits	
Packet size		Packet sequence number	
Msg type	Validity	Message size	
Originator address			
TTL	Nb hops	Message seq. number	
Reserved		Emission interval	Willingness
Link code	Reserved	Sub-message size	
Interface address			
Interface address			
…			
Reserved		Emission interval	Willingness
Link code	Reserved	Sub-message size	
Interface address			
Interface address			
…			

etc…

Figure 2.4 : HELLO packet format

2.2.3 Message TC (Topology Control)

These messages are flooded in the network (i.e. relayed by the set of MPR of the sender or previous relayer) and spread information on the network topology so as to build routing tables.



32 bits

8 bits	8 bits	16 bits
Packet size		Packet sequence number
Msg type	Validity	Message size
Originator address		
TTL	Nb hops	Message seq. number
ANSN		Reserved
Neighbor 1 primary address		
Neighbor 2 primary address		
…		

Figure 2.5 : TC packet format

In this message are listed the neighbors the original wanted to publish and that allow to reach the original sender. They also contain a sequence number (ANSN) incremented at each topology change so as to use only the latest data to perform updates.

2.2.4 HNA message (Host and Network association)

These messages allow performing routing operations between the ad hoc network and other networks that don't implement OLSR.

2.3 OLSR IN A NUTSHELL

The behavior of OLSR may sound complex. In fact it results of the superposition of three main components: neighborhood detection, MPR election and routing table computation. Those mechanisms are described in the following paragraphs.

2.3.1 NEIGHBORHOOD DETECTION

This mechanism uses the HELLO messages which are not retransmitted. Using this data, a node can learn:

- the primary address of its neighbors (from the originator address of received HELLO messages)
- the list of two-hop neighbors and the link type to the neighbors and two-hop neighbors (from the link type fields and list of associated addresses)

The following method is used to perform topology detection:

- An arriving node sends an empty HELLO
- Its new neighbors learn its primary address and learn the existence of an unidirectional link from the originator to themselves
- While receiving HELLO from its new neighbors, the arriving node learn their primary addresses and the existence of a symmetric link
- With the next HELLO sent by the arriving node, its neighbors reckon the link as symmetric.

After several HELLO exchanges, each node has a correct image of its neighborhood and can proceed to MPR election.

2.3.2 MPR ELECTION

Each node independently elects a set of MPR among its symmetric neighbors. The set of MPR is computed so that all symmetrical two-hop neighbors are reachable from the originator node through one of its MPR, while minimizing the number of elected MPR.

The RFC 3626 document describes the standard MPR election process:

- All symmetric neighbors with the highest willingness (WILL_ALWAYS) are elected as MPR
- All symmetric neighbors that are the only one able to reach a symmetrical two-hop neighbor of the originator are selected as MPR
- While all symmetric two-hop neighbors are not covered by at least one MPR, the symmetric neighbor with the highest willingness, or covering the most symmetric two-hop neighbors or having the highest number of neighbors itself is selected as MPR.

This mechanism is illustrated for an example of topology in the figure below.

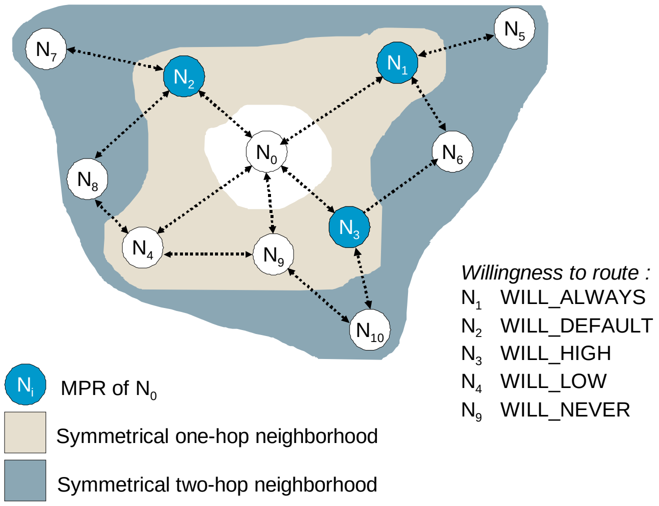


Figure 2.6 : Network after MPR election by N0

This mechanism is applied by all nodes, which yield to a connected graph of MPR in the network. This graph is used as support for broadcasting. Unicast packets require the computation of routing tables, which is described in the following paragraph.

2.3.3 ROUTING TABLE COMPUTATION

As the MPR graph is connected, a link composed of MPR only offers a minimal path from and to any point in the network. So, not only links have to be advertised. After the MPR computation process, each node sends, in a TC message, a list of neighbors he wants to publish (at least the list of all neighbors who have chosen itself as MPR).

Those message being flooded, each node can store a list of all nodes in the network and a list of links to these nodes, and thus build hop by hop a path to the destination.

3. SIMULATION FRAMEWORK

This section describes the framework used to simulate the test scenarios for performance measurements and the architecture of the nodes involved in the simulation.

3.1 OMNET++ AND THE MOBILITY FRAMEWORK

For this work, the OMNeT++ simulation tool was selected. It is a discrete time, event-based network simulator, where the nodes and components communicate by echanging messages that can figure actual data packets or internal messages.

The program is developped in C++ and extends the language object model by defining hierarchical modules, which allows a large flexibility in the design of complex nodes into a given network.

So as to manage mobility of the nodes an ad-hoc routing, OMNeT++ is extended with the Mobility Framework, whose implementation gives a dynamic management of connectivity and mobility of the nodes along with a support for a wireless channel model.

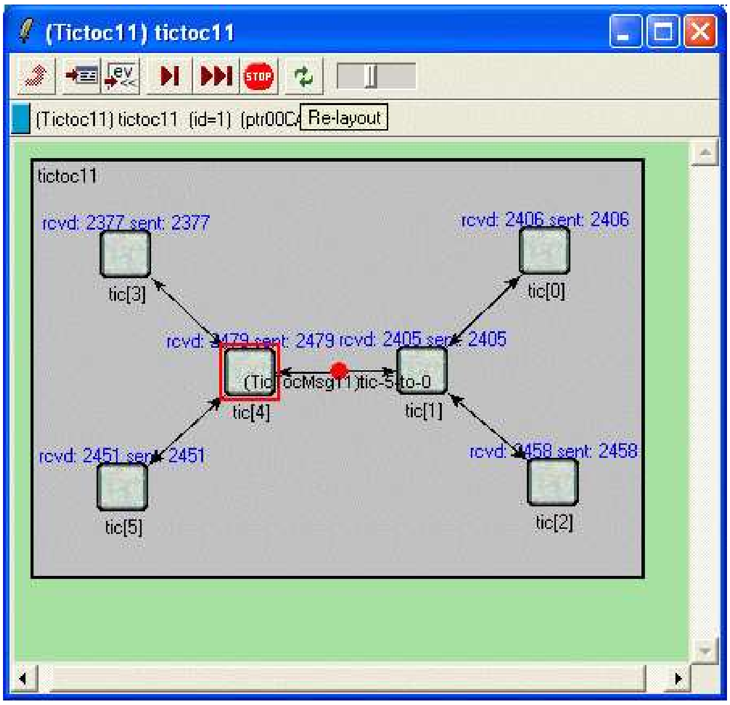


Figure 3.1 : OMNeT++ simulation environment

3.2 SIMULATION DESIGN AND IMPLEMENTATION

The architecture of the nodes used to simulate the behavior of the tested waveform rely on the use of several modules directly coming from different framework, like the mobility framework, or have been developed specially for this simulation.

The overall design of a node is showed on the figure below and further described in the following paragraphs.

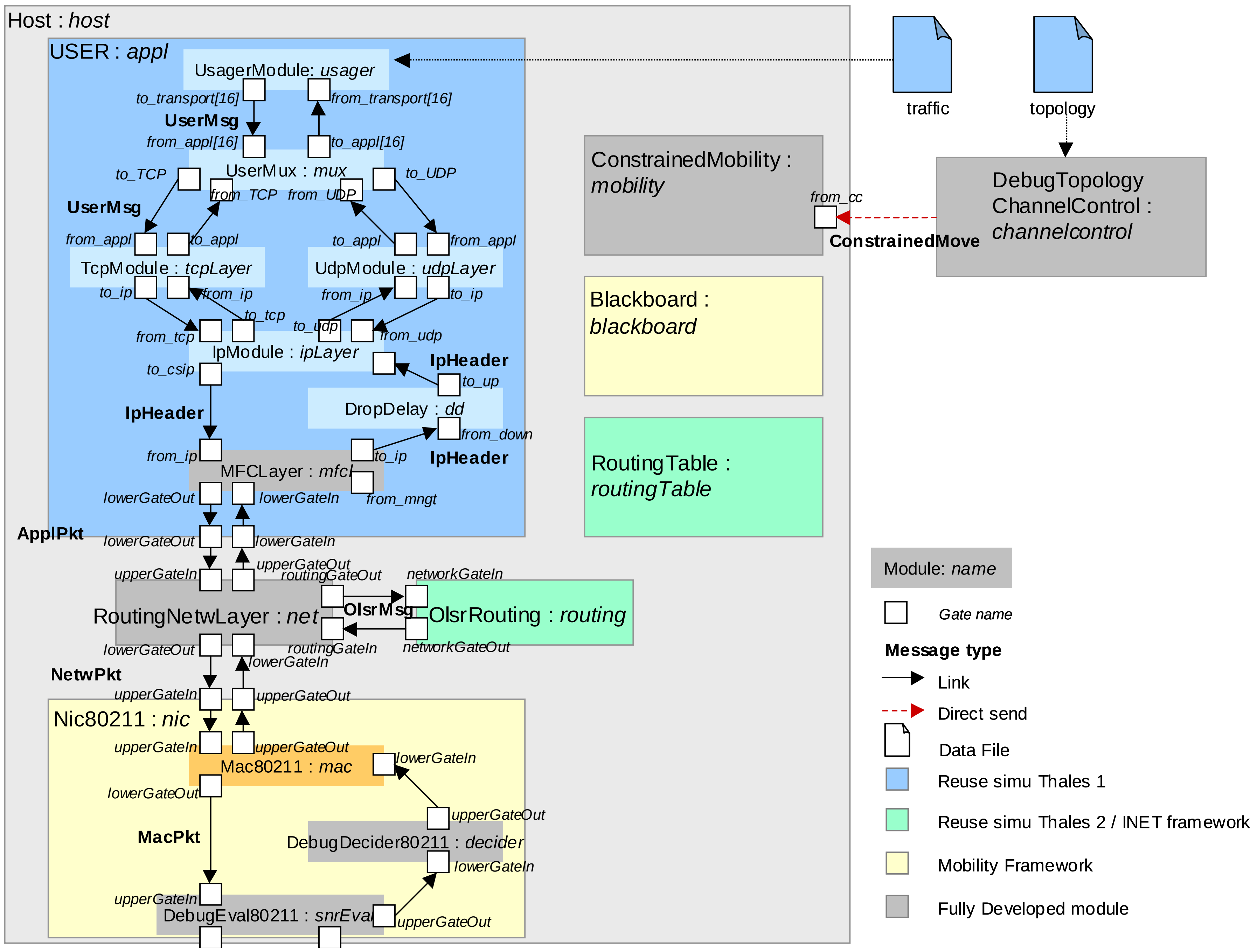


Figure 3.2 : Simulation architecture

3.2.1 Traffic generator

Traffic generation is handled by the USER module, implemented by each node in the network. It allows to insert into the network different flow, on TCP or UDP, and to simulate the use of different applications like file transfer via FTP, web browsing and voice and video over IP.

The traffic generator was initially developed for other simulations but was largely modified so as to integrate well into the current architecture using the mobility framework.

3.2.2 Mobility management

Mobility management relies on the principle introduced by the mobility framework. In this structure, mobility is handled in a distributed manner: each node can have its own mobility model and moves independently from each other, without knowing the position of the other nodes.

As a counterpart, after each movement, a node will update its coordinates to the ChannelControl module, which registers the positions of all the nodes in the network. By using a given physical propagation model, this omniscient module updates connections between nodes (which represent that the nodes are interfering rather than are “connected” at upper layers).

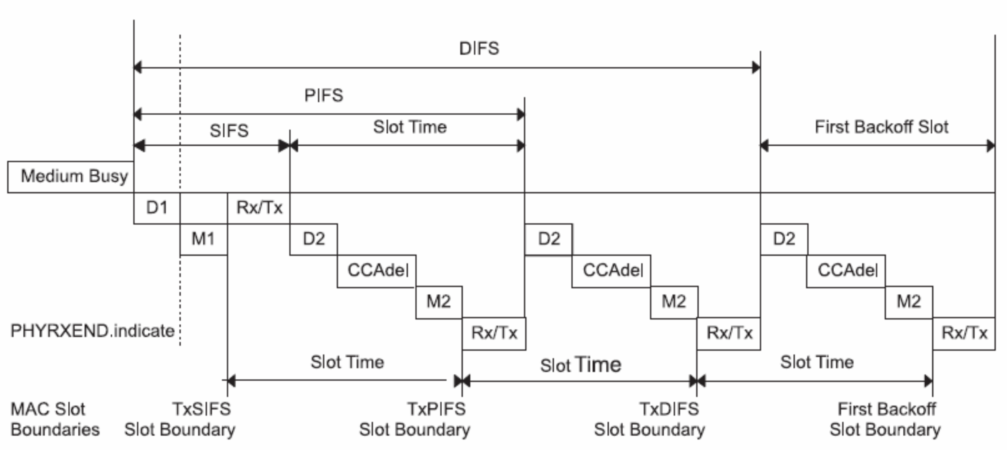
3.2.3 Data routing

Routing tables filling and updates are handled by the OLSR routing protocol. In the context of this work, the behavior of the protocol is simulated by the module OlsrRouting which updates the content of the RoutingTable model. The OlsrRouting module is a portage of the OLSR Unik implementation to OMNeT++ and is interfaced with the mobility framework using the RoutingNetwLayer module.

3.2.4 Channel access

The medium access control layer is based on CSMA/CA with the RTS/CTS option, as described in the IEEE 802.11 standard. However, this standard was defined for a transmission range of a few hundred meters, really different from the tactical communication transmission distances, which typically go up to 20 or 30 km. Besides, the data rate of those communications are limited to around 500 kbits/s

Therefore some adaptations had to be made to the standard, particularly concerning the inter-frame spacing durations. Those durations are most of the time given without any justification in the literature and only a thorough reading of the IEEE original document allow to have a detailed description of their calculation.



D1 = aRxRFDelay + aRxPLCPDelay (referenced from the end of the last symbol of a frame on the medium)
D2 = D1 + Air Propagation Time
Rx/Tx = aRXTXTurnaroundTime (begins with a PHYTXSTART.request)
M1 = M2 = aMACPrcDelay
CCAdel = aCCA Time - D1

Figure 3.3 : Inter-frame spacing details

The interesting duration are tslot and SIFS (short inter-frame spacing) as all the other durations are computed from those two values. They are defined as :

$$t_{slot} = aCCATime + aRxTxTurnaroundTime + aAirpropagationTime + aMACprocessDelay \quad \textbf{(eq. 3.1)}$$

$$SIFS = aRxRFDelay + aRxPLCPDelay + aAirpropagationTime + aMACprocessDelay \quad \text{(eq. 3.2)}$$

By knowing the transmission and carrier sensing ranges required for the tactical waveform and the physical properties of the material (like the time for the transceiver to switch from receive to transmit mode), it is possible to compute the appropriate values for the inter-frame spacing durations. Those results are shown in the table below.

Tableau 3.1 : Inter-frame spacings for the IEEE 802.11 standards and the tactical waveform

	802.11b	802.11g	Tactique Hdw	Tactique Sftw
tslot	2,000E-05	9,000E-06	1,552E-04	1,153E-03
SIFS	1,000E-05	1,600E-05	4,700E-05	1,045E-03
DIFS	5,000E-05	3,400E-05	3,575E-04	3,351E-03
TX_range	250	250	15000	15000
PCS_range	550	550	30000	30000
AirPropagTime	1,835E-06	1,835E-06	1,001E-04	1,001E-04
RxRFDelay	2,500E-06	2,500E-06	2,500E-06	2,500E-06
RxPLCPDelay	2,500E-06	2,500E-06	2,500E-06	2,500E-06
MACProcessingDelay	0,000E+00	2,000E-06	2,000E-06	1,000E-03
RxTxTurnaroundTime	5,000E-06	5,000E-06	*Confidentiel*	*Confidentiel*
CCATime	1,317E-05	4,000E-06	*Confidentiel*	*Confidentiel*

The two different values for the tactical waveform are obtained considering that the MAC processing functions are handled by hardware (dedicated chipset or FPGA) or by a software layer whose processing time is much longer.

In both cases, the adaptation of the inter-frame durations are really penalizing during the phases of contention for the channel access. In the simulations, the assumption of a dedicated hardware for MAC processing has been made.

3.2.5 Radio channel modeling

The radio channel model used should be able to show the limitation of the channel access control used but remain simple enough not to create additional artifacts that may make the obtained result hardly understandable.

In the simulation framework, the description of the radio channel model is implemented in the ChannelControl module and in the lower layer of each node (Mac, Decider and SnrEval modules).

The selected model used two main ranges :

- A transmission range (TX_range) where all emitted packets are received without loss and error. However, several emitted packets in this range may collide;
- An interference range (IF_range) where emitted packets cannot create collision but occupy the channel. This range is similar to a carrier sensing range but is named interference range to stay coherent with the mobility framework denominations.

The tactical waveform simulated being reinforced against jamming and packets collision, we can estimate that a frame is still understandable if less than its half has been subject to collision or interference (except if this happens on the first 80 bits which are used for synchronization).

4. Simulation and results analysis

This section describes an example of simulated scenario of mobility and traffic and gives a detailed analysis of the results. Some conclusion on the behavior of the simulated waveform and some ideas of improvements are also presented.

4.1 An operational scenario: securing Brinon

This scenario assesses performances in an operational scenario in which several units with different missions (artillery, motorized infantry, recognition units ...) have a common objective: securing the city of Brinon. This allows testing different services offered by the waveform (initialization and merging of networks, adaptation of routing to topology changes).

4.1.1 Scenario detail

During this scenario, recognition units, assisted by military engineering will first go to the objective. Motorized infantry and tanks will create a secured zone in the south of the city while the artillery will cover the operation from the rear of the battlefield. The first node figures the headquarters and stays still during the whole operation.

The mobile nodes will exchange situation awareness information all along the scenario. Besides, node 2, as a recognition node will emit a point to multi-point voice over IP flow (simulated by N point to point flows) to some other nodes in the network (including node 1). Finally, a FTP session is established between nodes 2 and 7 and between nodes 3 and 8.

The transmission range has a radius of 7km and a carrier sensing range of 14km is used. Besides, the emitted frames are supposed to resist up to 50% of interference and collisions.

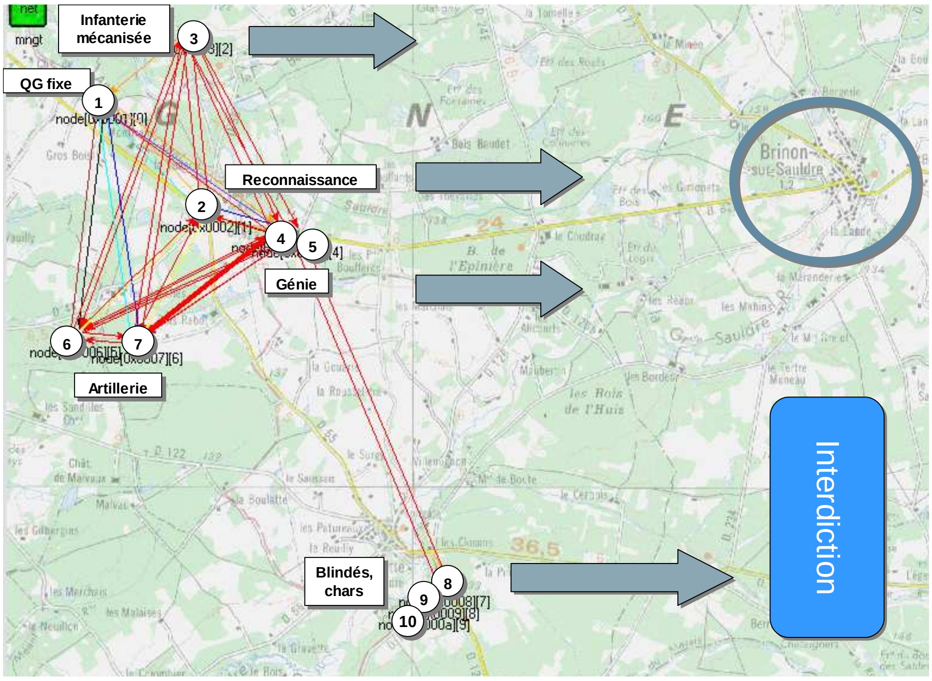


Figure 4.1 : Map of the simulated scenario

4.1.2 Results and analysis

The results obtained with the previously described scenario are transcribed in the table below, which presents UDP traffic only (situation awareness and voice over IP).

Tableau 4.1 : Simulation results for UDP traffic

Traffic type	*S.A*	*VoIP*	*Total*
Submitted traffic (kbits/s)	3,637	76,816	80,453
Received traffic (kbits/s)	3,542	43,171	55,722
Ratio	0,974	0,562	0,581
Average delay (s)	0,129	0,204	0,186
Maximum delay (s)	24,80	3,384	24,80
Jitter (s)	0,240	0,072	0,112
Collisions (in packets)	-	-	5531
Drops on full MAC queue	-	-	121137
Drops on max. retransmissions	-	-	414
Drops on routing error	-	-	23238
OLSR overhead (kbits/s)	-	-	4,83

The situation awareness traffic sees satisfying performances (98% of the packets are correctly received) and the delays are correct for this type of application (less than 130ms in average).

However, the simulation shows insufficiencies in the network behavior concerning the voice over IP flows. Those packets are correctly received only in a limited fraction (less than 60%) and experienced latency is far too high for this interactive application (200 ms in average).

Besides, and despite the fact that the average data may seem acceptable, a thorough analysis of the results reveals an important disparity between the different flows, as the figure below shows it.

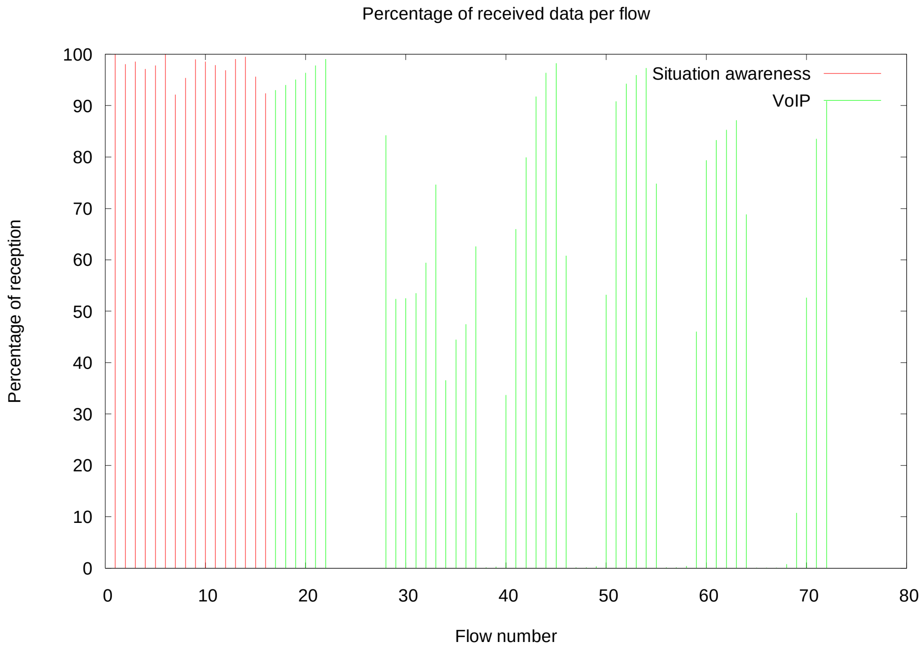


Figure 4.2 : Percentage of received packets for different flows

The analysis of the size of the MAC queues of the different nodes, illustrated by the next figure, reveals that, as soon as the different voice over IP sessions start, the node 2 is saturated as it generates or relays too much traffic.

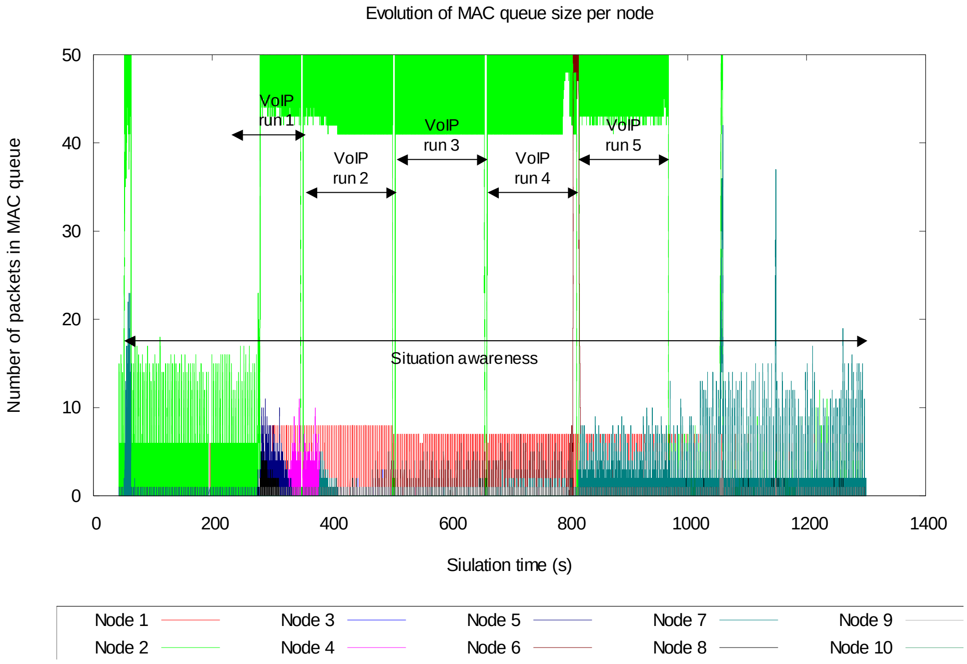


Figure 4.3 : Evolution of the MAC queue sized during simulation

One of the main interrogations comes from the fact that similar situations have been encountered in different scenarios involving a important voice over IP traffic originated or transiting by a single node.

Those experiments allow to put in light a major limitation of the CSMA/CA channel access control mechanism when it uses the RTS/CTS mechanism. A calculation of the overhead due to the use of control packets and the modified inter-frame durations, when used with voice over IP traffic (a 32 bytes datagram emitted every 30 ms) yields the following result: the efficiency of the MAC layer for VoIP is below 20%.

Therefore, the theoretical throughput of the channel being around 500 kbits/s, a single node can only carry around 100 kbits/s of user traffic for voice over IP flows. In this scenario, the load is so high that this limit is reached and the node 2 is not able to send or relay this amount of traffic, and therefore is the place of many packet losses.

The following ideas are suggested so as improve performances and correct to some extent the limitations of the network:

- Enabling multicast, so the VoIP flows would be sent only once from node 2 to its neighbor, and therefore reduce the use of the RTS/CTS mechanism which has been reckoned very penalizing;
- Aggregating packets, so as to avoid sending a lot of very small packets and therefore limit the MAC layer overhead, at the price of an inflated latency in packet delivery;

- Prioritizing VoIP flows, using recent QoS improvements to the IEEE 802.11 standard, like 802.11e which introduces a contention free bursting period where the VoIP could be sent.

- Load-balanced routing, so as to avoid whenever possible to overwhelm a node with traffic and find different paths, where nodes are more lightly used.

The observed TCP flows have a throughput of around 50 kbits/s which is far below from the observed values under light load. TCP is known to yield throughput to different UDP traffics. Here, this phenomenon is emphasized by the load of node 2. It is therefore important to introduce a load-balanced routing so as to spread as much as possible the traffic across nodes of the network (and, for example, find a longer path but less loaded for the TCP flows).

Finally, the behavior of the OLSR routing protocol is satisfying. The network only counting a few nodes, lightly meshed, the overhead of the protocol is limited to 4.83 kbits/s. The neighborhood computed by the protocol is very close to the actual topology, as shown on the protocol below.

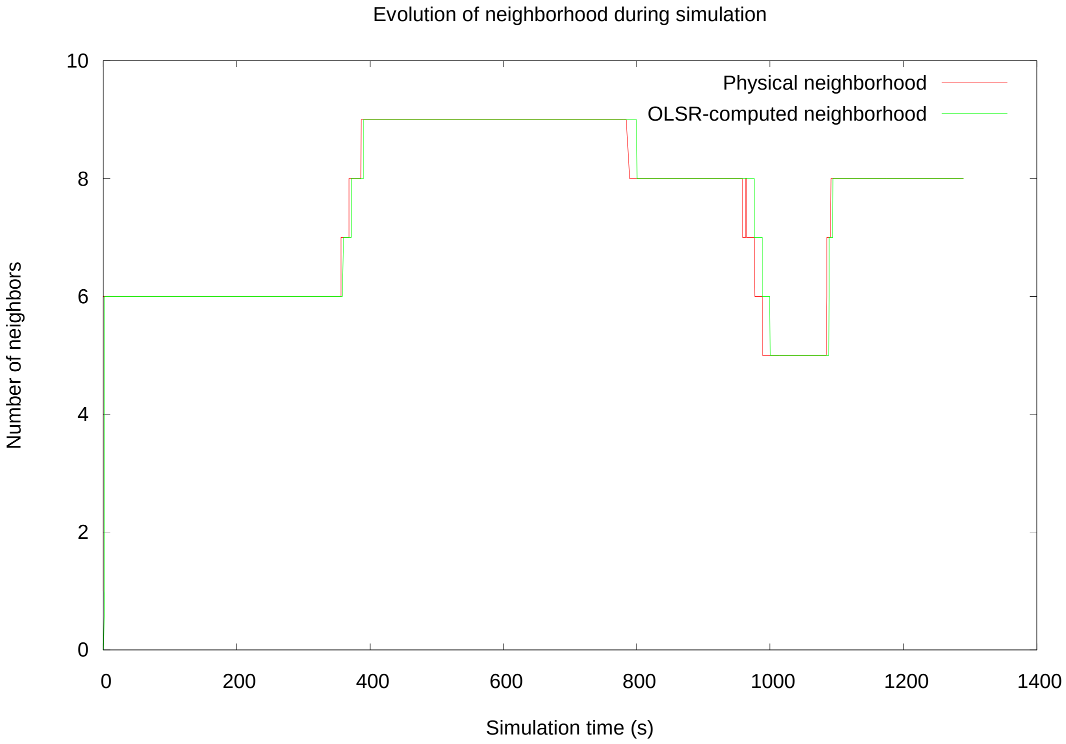


Figure 4.4 : Evolution of the neighborhood of node 2 during the simulation

4.2 Synthesis of results

The previous scenario and other studies allowed to draw a list of strengths and weaknesses of the developed contention-based waveform and to suggest some improvements that are currently at a development stage.

Tableau 4.2 : Synthesis of performances and suggested improvements

Item	Contention-based waveform	Suggested improvements
Channel Access Control		
Type	CSMA/CA Contention access	Load-balanced routing *Contention Free Bursting* (cf. 802.11e standard) Packet aggregation
Advantages	Statistically equitable access to the channel No allocation to unused links	
Drawbacks	Starvation for exposed nodes Important overhead for small packets	
Routing		
Type	Proactive (OLSR)	Prioritized routing flows OLSR improvements (*fish-eye*, *cross-layering*) Multicast management
Advantages	Good mobility handling Slow latency at route establishment	
Drawbacks	Disturbed behavior at high load Important overhead (depending on the network size and topology)	
Throughput		
Advantages	Good performances of TCP Reliable under low load	CSMA/CA multi-channel extension QoS routing
Drawbacks	Collapsing of performances at high load Interaction between flows	
Latency		
Advantages	Very low at light load	Introduction of fast forwarding circuits for flows with latency constraints
Drawbacks	Large jitter Latency not bounded	

The contention-based waveform, using CSMA/CA for channel access control and OLSR as a routing protocol, seems to perform well under a limited load a when the network topology allow the optimizations of the routing protocol to express fully. However, tactical communications require a high reliability, whatever the utilization constraints and the network topology may be. As a consequence, this waveform is hardly usable in a tactical context without any of the improvements suggested above.

However, all the measurements realized here have proved very useful so as to obtain a better understanding of all the mechanisms involved in the behavior of such a network and to have reliable comparison points with other waveform, using different approaches, developed by Thales.

5. CONCLUSION

This internship was for me a good opportunity to extend my knowledge in the field of wireless and ad-hoc networks, and particularly concerning the use of the latter in tactical communications.

The first phase of my work allowed me to deepen my theoretical knowledge on the area (detailed behavior of CSMA/CA, of the OLSR routing protocol, introduction of quality of service with 802.11e). Then, by implementing and analyzing several simulations, I could comfort this with practical results.

The process of designing and implementing the simulation environment, with all the associated modeling process appeared very interesting to me. Judiciously choosing the components to model and the way to model it, is a difficult but very intellectually gratifying task, that allow to understand better the mechanisms of wireless networks.

From a personal point of view, I acquired a significant experience during this internship, both in the field of ad-hoc networks and concerning the management of large project in an international company, and this will help me in my future professional career.

REFERENCES

[1] P. Jacquet, P. Mühlethaler, T. Clausen, A. Lauoiti, A. Qayyum, L. Viennot. *Optimized Link State Routing Protocol for Ad-hoc Networks*.

[2] T. Clausen, P. Jacquet. *RFC 3636, Optimized link-state routing protocol*.

[3] A. Laouti, P. Mühlethaler A. Najid, E. Plakoo. *Simulation Results of the OLSR Routing Protocol for Wireless Network.*

[4] T. Clausen, G. Hansen, L. Christensen, G. Behrmann. *The Optimized Links State Routing Protocol Evaluation through Experiments and Simulation*.

[5] P. Kuosmanen. *Classification of Ad-hoc Routing Protocols.*

[6] C. Siva Ram Murthy, B. S. Manoj. *Ad-hoc Wireless Networks, Architectures and Protocols*. Prentice Hall.

[7] M. Benzaid, P. Minet, K. Al Agha. *Integrating fast mobility in the OLSR routing protocol.*

[8] M. Benzaid, P. Minet, K. Al Agha. *Analysis and simulation of Fast-OLSR.*

[9] J. Schiller. *Mobile Communications, Second Edition.*

[10] M. Gast. *802.11 Réseaux sans fil, La référence*.

[11] S. Basagni, M. Conti, S. Giordano, I. Stojmenovic. *Mobile Ad-hoc Networking*.

[12] S. Xu, T. Saadawi. *Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad-hoc Networks?*

[13] C. T. Calafate, P. Manzoni, M. P. Malumbres. *Assessing the effectiveness of IEEE 802.11^e in multi-hop mobile network environments.*

[14] J. del Prado Pavón, S. Shankar N. *Impact of Frame Size, Number of Stations and Mobility on the Throughput Performance of IEEE 802.11e.*

[15] A. Leon-Garcia, I. Widjaja. *Communication Networks : Fundamental Concepts and Key Architectures, Second Edition*.

[16] A Kanzaki, T. Uemukai, T. Hara, S. Nishio. Dynamic TDMA Slot Assignment in Ad-hoc Networks.

[17] C.D. Young. *USAP : a unifying dynamic distributed multichannel TDMA slot assignment protocol*.

[18] C.D. Young. USAP multiple access : dynamic resource allocation for mobile multihop multichannel wireless networking

[19] A. Varga. OMNeT++ Manual. March 2005.

[20] M. Löbbers, D. Willkomm. A Mobility Framework for OMNet++, User Manual.

[21] Xiaoyan Hong, Kaixin Xu and Mario Gerla. Scalable Routing Protocols for Mobile Ad Hoc Networks. July 2002.

[22] ANSI/IEEE Standard 802.11, 1999 Edition (R2003). June 2003.