Quality of service support, security and OSPF interconnection in a MANET using OLSR

Cedric Adjih, Pascale Minet, Paul Muhlethaler, Emmanuel Baccelli, and Thierry Plesse

Abstract— The MANET networks are of prime interest for military networks. One of the proeminent routing protocols for MANET is OLSR, and indeed, OLSR has been used in many evaluations and experiments of MANETs. As OLSR is on its way to standardization, there are still a number of extensions that are useful and sometimes necessary for practical use of OLSR networks: such extensions are quality of service support, security, and OSPF interconnection. In this paper, we present the architecture, design, specifications and implementations that we made to integrate these features in a military test-bed. This test-bed is a real MANET comprising 18 nodes. These nodes communicate by radio and use the IEEE 802.11b MAC protocol. The OLSR routing protocol updates the routing table used by the IP protocol to forward packets.

Keywords— mobile ad hoc networks, OLSR, quality of service, security, OSPF, interconnection.

1. Introduction

A mobile ad hoc network (MANET), is a collection of autonomous mobile nodes communicating over a wireless medium without requiring any pre-existing infrastructure. These nodes are free to move about arbitrarily. MANETs exhibit very interesting properties: they are self-organizing, decentralized and support mobility. Hence, they are very good candidates for tactical networks in military applications. Military world integrates today new concepts which are, i.e., battlefield digitalization (NEB), network centric warfare (NCW), aeroterrestrial operational bubble (BOA), cooperative engagement. The goal of these concepts is to create a total numerical network, amongst other things on tactical perimeter, which connects the various tactical pawns (i.e., headquarters, soldiers). In the general context of military IP networks architecture (strategic, operative, tactical), with implementations on various types of technological supports, and through various networks (i.e., fixed, mobile, satellite), it is required for a MANET to be a full IP network. As a MANET is generally multihop, and in order to allow the communication between any two nodes, a routing protocol must be used. The IETF MANET working group has standardized four routing protocols that create and update the routing table used by IP. Among them, optimized link state routing (OLSR) [1] is a proactive protocol where nodes periodically exchange topology information in order to establish a route to any destination in the network.

The OLSR [1] is an optimization of a pure link state routing protocol. It is based on the concept of *multipoint relays* (MPRs). First, using multipoint relays reduces the size of the control messages: rather than declaring all its links in the network, a node declares only the set of links with its neighbors that have selected it as multipoint relay. The use of MPRs also minimizes flooding of control traffic. Indeed only multipoint relays forward control messages. This technique significantly reduces the number of retransmissions of broadcast messages. Each node acquires the knowledge of its one-hop and two-hop neighborhoods by means of periodic *Hello* messages. It 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 its two-hop neighbors. Each node also maintains topological information about the network obtained by means of *topology control* (TC) messages broadcast by MPR nodes. The routing table is computed by the Dijkstra algorithm. It provides the shortest route (i.e., the route with the smallest hop number) to any destination in the network. In [2], we reported the performance evaluation results showing that a MANET with OLSR routing achieves very satisfying performances.

However, OLSR, as defined in [1], does not support quality of service (QoS) and hence does not satisfy the military operational constraints associated with the various traffics exchanged in a tactical mobile ad hoc network. On these tactical mobile networks, as on the fixed networks, various types of traffics coexist: data, voice, and video. These traffics have different characteristics and military operational constraints. They must receive a differentiated treatment: the importance of military operational flows (i.e., hierarchical priority) must be taken into account (example: "flash" message crossing a mobile ad hoc network). The QoS support based on OLSR has to take into account constrained environments and to optimize with respect to this environment, the mechanisms which contribute to QoS support. The concept of constrained environments can correspond to various operational military criteria such as low data bit rate, "time constrained network", secured architecture of "red/black" type, constraints of mobility. It is also necessary to manage end-to-end QoS in an optimal way, to correlate IP level quality of service with that of the radio level. That leads, among other things, to the optimization of the couples "QoS mechanisms – radio medium access protocol (MAC layer)": concept of "cross layering".
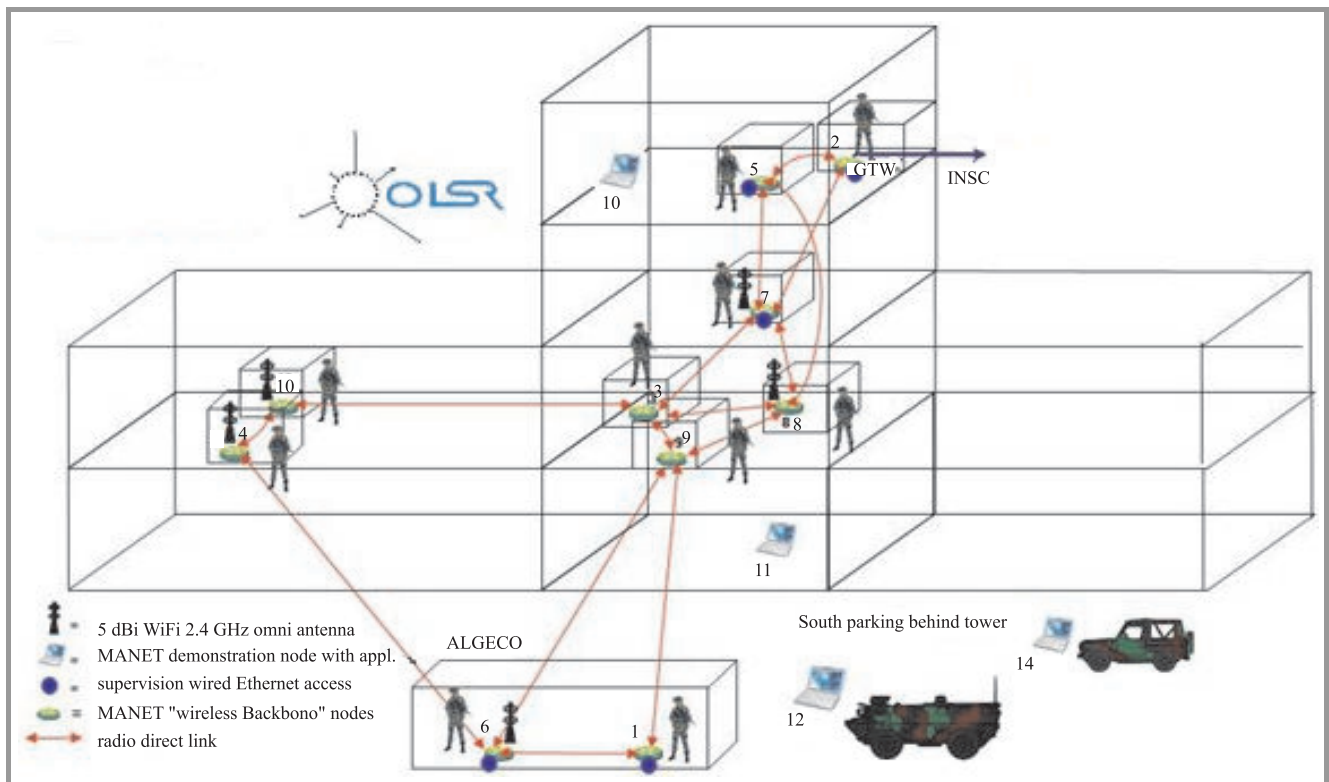
70

Fig. 1. The CELAR MANET/OLSR platform. Explanations: ALGECO – a modular construction, INSC – interoperable networks for secure communications.

We present a QoS support based on OLSR in Section 2. Another requirement in a military network is security. The OLSR routing protocol, as defined in [1], does not meet this requirement. Indeed, a node can, for instance, pretend to be another node or advertise false links. Such a behavior can seriously damage the routing. In extreme cases, no message reaches its destination. This problem is common to both reactive and proactive routing protocols. That is why, we have proposed mechanisms to provide a secure routing. These mechanisms will be presented in Section 3.

A tactical network is not isolated, it should be able to communicate with other networks, more conventional. These networks generally use open shortest path first (OSPF). Consequently, an interconnection should be done between the OLSR and the OSPF routing domains. We show how to take advantage that both protocols are link based routing protocols in order to perform such an interconnection. This OLSR-OSPF interconnection is described in Section 4.

The MANET in general and OLSR networks specifically, are of prime interest to DGA/CELAR (French MoD). Hence in partenership with INRIA, which developped and installed a MANET/OLSR platform at CELAR (Technical Defense Center for Information Warfare), such OLSR-based MANETs have been experimented and their features and performances have been evaluated.

The platform used for experimentation is illustrated by Fig. 1. It comprises 18 nodes which are routers, laptops and VAIOs. They use the IEEE 802.11b protocol to access the wireless medium. They operate with IPv4 or IPv6. They use the OLSR protocol for routing. This protocol has been enhanced with security functionalities and QoS support. The nodes are distributed in the central tower of the CELAR, and in a shelter, denoted ALGECO on Fig. 1, and some of them are embedded in vehicles. This MANET is interconnected to a wired network by means of an OLSR-OSPF router. This router takes advantage of the fact that both routing protocols are link-state protocols.

In this paper, we describe in Section 2 the QoS support we have implemented on this platform. We will present in Section 3 how to make the OLSR routing protocol secure. Section 4 shows how to interconnect an OLSR routing domain with an OSPF one, taking advantage of the fact that both are link state routing protocols.

2. QoS support in an OLSR MANET

Several works deal with QoS support in a MANET, see for instance [3–6]. Some of them are based on the OLSR routing protocol like [7–10]. The QoS support we have implemented on the CELAR platform comprises five components as illustrated by Fig. 2.

As resources are scarce in MANETs, our extension [10] keeps the optimizations present in OLSR, which rely on two principles:

– a partial topology knowledge: the advertised link set is a subset of the whole topology;

Cedric Adjih, Pascale Minet, Paul Muhlethaler, Emmanuel Baccelli, and Thierry Plesse

– an optimized flooding, called MPR flooding: it is based on the concept of multipoint relays.

In this solution, we distinguish the four following **classes of flows**, listed by decreasing priority order.

- **Control flows**. They are required to make the network operational, like for instance OLSR messages. This class is not allowed to user flows.

- **Delay flows**. These flows have delay requirements, like voice flows. In this solution, they are processed with a high priority.

- **Bandwidth flows**. These flows have bandwidth requirements, like video flows.

- **Best effort flows**. They have no specific QoS requirements.

In the following, we denote QoS flows, flows having delay or bandwidth requirements. BE denote best effort flows.
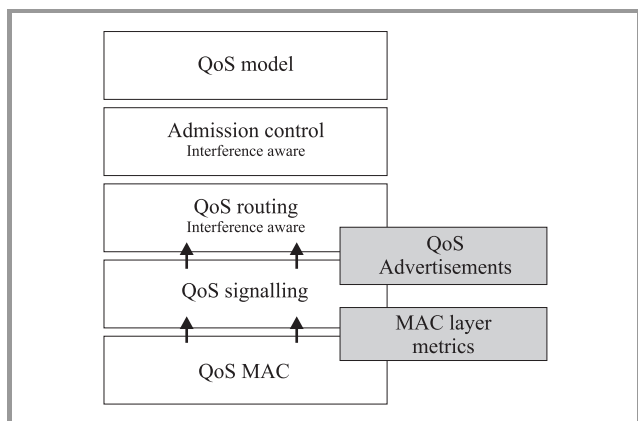

Fig. 2. The QoS support with its five components.

The admission control is in charge of deciding whether a new QoS flow can be accepted or not. The decision depends on the bandwidth requested by this flow, the available bandwidth at each node and the possible interferences created by this flow. If there is not enough resources to accept the new flow, this flow is rejected. The decision is taken locally by the source of the QoS flow with regard to the bandwidth requested by the flow.

We can notice that this admission control is applied only on QoS flows. If BE flows were not constrained, they could saturate the medium and degrade the QoS granted to QoS flows. We introduce a leaky bucket on each node to limit the bandwidth consumed by BE flows and protect the QoS flows.

To select the shortest route meeting the bandwidth required, the QoS routing protocol must know the bandwidth locally available at each node. QoS signalling is introduced for that purpose. QoS parameters values are disseminated in the network by means of MPRs. The selection of MPRs

is modified to consider the bandwidth locally available at each node. The main drawback of this solution lies in the overhead generated. Each flooded message leads to a number of retransmissions higher than that obtained with native OLSR [10]. In order to conciliate the optimized performances of MPR flooding with QoS support, we distinguish two types of MPRs.

- The MPRs, selected according to the native version of OLSR, are used to optimize flooding.

- The QoS MPRs, selected considering the local available bandwidth, are used to compute the routes.

This extension of OLSR would provide better performances if a QoS MAC were used. An ideal QoS MAC would be deterministic, would grant access to the waiting packet with the highest priority and would provide information concerning the QoS at the MAC level (example: the local available bandwidth, the waiting time for transmission). However, even if the MAC layer does not support QoS, QoS OLSR improves the quality of service provided to QoS flows, as shown in [10, 11], where the protocol used is IEEE 802.11b.

We can notice that this QoS support does not need any additional message. The *Hello* and TC messages of OLSR are extended with QoS information in order to allow any flow source to compute the shortest route providing the bandwidth requested by its new flow. As the problem of finding a route meeting a given bandwidth has been shown NP-hard in wireless networks subject to radio interferences [4], we use an approximation to compute the bandwidth consumed by a flow at the MAC level. This approximation is used only by the QoS routing protocol to select the route which also depends on the local available bandwidth measured at each node. Once a route has been found for a QoS flow, it is used by all packets of the flow considered, until either a shorter route is established because network resources have been released, or it is no longer valid because of a link breakage. Source routing can be used for that purpose. Notice that BE flows are routed hop-by-hop.

With this QoS support, QoS flows receive a throughput close to this requested, their delivery rate is improved, because interferences are taken into account. Users perceive the QoS improvement. Moreover, this gain is still obtained in case of node mobility up to 20 m/s. In that case, some additional rules should be taken in the selection of MPRs and QoS MPRs, in order to avoid nodes at the transmission range limit.

3. Security in an OLSR MANET

A significant issue in MANETs is that of the integrity of the network itself. OLSR allows any node to participate in the network – the assumption being that all nodes are behaving well and welcome. If that assumption fails,

then the network may be subject to malicious nodes, and the integrity of the network fails.

In OLSR as in any other proactive MANET routing protocol, each node must, first, correctly generate routing protocol control traffic, conforming to the protocol specification. Secondly, each node is responsible for forwarding routing protocol control traffic on behalf of other nodes in the network. Thus incorrect behavior of a node can result from either a node generating incorrect control messages or from incorrect relaying of control traffic from other nodes. Thus we have two types of attacks against the OLSR routing protocol.

The first type of attack consists, for a node, in generating incorrect control message. For this first type of attack, the node can generate a fake control message from scratch or it can replay already sent control messages. In this second case, we have an incorrect control message generation using replay. Another even more advanced such replay attack consists in capturing a control message in a given location of the network and relaying it very rapidly to another location to replay it.

In the second type of attack, the node is not relaying correctly either the control messages or the data packets. This attack can range from the absence of relaying to an incorrect relaying, e.g., a data packet can be forwarded to a wrong next hop node.

The security architecture initially proposed in [12] that we have used to counter the previous attacks relies on two main mechanisms:

- a signature mechanism is used to authenticate control messages;

- a timestamp mechanism is used to ensure the freshness of control messages.

This security architecture can be easily implemented using the message format shown in Fig. 3. Notice that the optional source interface address is used to make the sig-
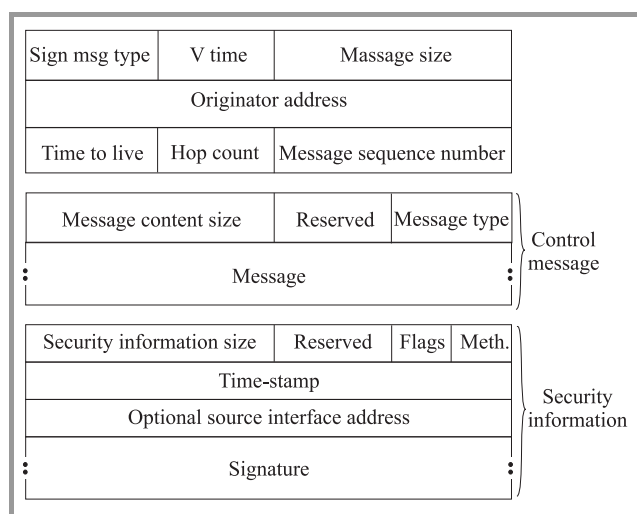
nature depends on this address which is not in the OLSR message; without this option attacker could replay a *Hello* message changing the source interface address which is found by OLSR in the IP header.

For the signature mechanism, three possibilities were considered.

- Signature with symmetric cryptography, traditional asymmetric cryptography or identity-based (pairing-based) cryptography.

- Using asymmetric keys (with traditional cryptography) requires the distribution of these keys: this leads to overhead and additional attacks.

- Identity-based cryptography (based on pairing) could be an interesting solution, however the signature and verification times are beyond the computational power of the routers (see [16]).

For simplicity and computational power reasons, we have implemented the HMAC authentication algorithm (which MD5 hashing function) using a symmetric shared secret key.

The timestamps are simply the times given by nodes internal clock. A strict synchronization of nodes clocks is not necessary since the timestamp is used to complete the already existing protection offered by the message sequence number and the duplicate set. As a matter of fact, messages that are already in the duplicate set are silently dropped.

If the nodes clocks are of very poor quality, it is still possible to use them to generate timestamps. In [17] an OLSR secure time protocol (OSTP) is presented. It allows nodes to run with non-synchronized clocks while the timestamps are still using the nodes clocks.

With such security architecture and without compromised nodes, the above mentioned attacks can be countered except the relay attacks. Attacker nodes will be maintained outside the network; these nodes will never be relays and will even not be present in the routing table of the network nodes. The relay attacks as the attacks in presence of compromised nodes are more difficult to counter; possible techniques are proposed in [13–15]. Compromised nodes have the knowledge of given crypotgraphic keys of the network.

4. OSPF interconnection

4.1. Overview

The OLSR and OSPF are both well-established protocols with different application areas. However in the military networks, at different levels, there are network infrastructures that fit the requirements of either OLSR or OSPF.

Hence, one important feature is to be able to integrate both types of networks and make them interoperate. A general

Sign msg type	V time	Massage size	
Originator address			
Time to live	Hop count	Message sequence number	
Message content size		Reserved	Message type
Message			
Security information size		Reserved	Flags	Meth.
Time-stamp			
Optional source interface address			
Signature			

Fig. 3. Format of a signed message.

solution is to use an external protocol such as border gateway protocol (BGP) [18], to connect networks with different routing technologies.

Fortunately, OSPF and OLSR share some similarities: they are both link state protocols. Hence a possibility exists to make both interoperate.

In this spirit, we indeed designed, implemented and experimented a mechanism to perform OSPF/OLSR interconnection. The core idea is the following: OSPF and OLSR both incorporate mechanisms in order to exchange routing information with other routing protocols; hence those mechanisms are used.

4.2. Principles of the OSPF/OLSR interconnection

The OLSR features a simple and efficient mechanism to import routes coming from another routing protocol: host and network association (HNA) messaging. With these messages, an OLSR node can advertise it has reachability to non-OLSR hosts or networks. For instance, if an OLSR node is also connected via another interface to an OSPF network, it can periodically generate and transmit such HNA messages including the OSPF network's IP prefixes. Routes to the OSPF network will then be included in OLSR-driven routing tables.

Similarly, OSPF features its own mechanisms to import routes coming from another routing protocol: link state advertisement (LSA) messages type 5 and 7. These messages advertise routes that are "external" to the OSPF network, which are then included in OSPF-driven routing tables. There are however two different types of metrics.

In order to achieve OLSR/OSPF interconnection, it is therefore sufficient to use these two mechanisms to transfer routes between OSPF and OLSR through the interface routers (the routers that have both OSPF and OLSR interfaces).

4.3. Implementation of the OSPF/OLSR interconnection

In practice, in OLSR and OSPF, the mechanisms to import route from other protocols are implementation-dependent. Hence, we started with the choice of two implementations: the OLSR implementation which is used is the OOLSR implementation [20] from INRIA.

The OSPF (OSPFv3) implementation which is used, is part of the Quagga [21] routing suite (precisely *quagga-0.99.4*). It is a derivative of Zebra [23]. Notice that we will use the names Zebra and Quagga interchangeably, since the architecture, interfaces and code are near identical.

The overview of Quagga, is given by supporting documentation [22]: *"Quagga is a routing software suite, providing implementations of OSPFv2, OSPFv3, RIP v1 and v2, RIPv3 and BGPv4 for Unix platforms, particularly FreeBSD, Linux, Solaris and NetBSD. The Quagga architecture consists of a core daemon: zebra, which acts as an*

abstraction layer to the underlying Unix kernel and presents the Zserv API over a Unix or TCP stream to Quagga clients. It is these Zserv clients which typically implement a routing protocol and communicate routing updates to the zebra daemon", … such as ospf6d, implementing OSPFv3 (IPv6).

Hence, the central part of Quagga, is the *zebra* daemon which is offering an API, called Zserv. This main daemon is in charge of actually performing low-level or system-level parts, such as for instance setting up the routes in the kernel. It is also in charge of exchanging routes, interfaces and addresses information to the daemons.

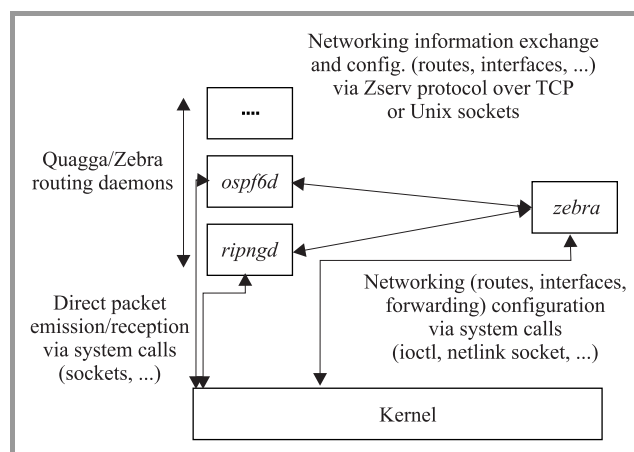Figure 4 represents the architecture of Quagga: each routing protocol is implemented as a daemon.

Fig. 4. Zebra/Quagga architecture.

As a result of running the routing protocol, some routes are detected or exchanged between some nodes in the network.

Instead of setting directly the routes as in traditional routing protocol implementations, the routing daemons communicate the added/deleted routes to the main daemon *zebra*, which will add/remove them actually in the network.

An important point is that the Zserv protocol between the main daemon and the routing protocol daemons includes the ability to send routes in both directions: hence, in Fig. 4, the *ospf6d* daemon is also able to get routes which are set up by *ripgngd* for instance, if it has registered to do so. This feature is largely used in the Quagga routing suite, in order for daemons to redistribute routes obtained by other daemons.

4.4. Interconnection between OOLSR and Quagga: QOED

In order to interconnect OLSR and OSPF, we have decided to use the traditionnal way of Quagga: another routing daemon is added, which sets routes by communicating with the main *Quagga* daemon. The exchange of routes between OLSR and OSPF is then done through this main daemon.

As shown on Fig. 5, the communication is actually done indirectly, using a daemon called *QOED, Quagga OOLSR Exchange daemon*, which mediates between Quagga and OOLSR. The reasons for this are multiple, but mostly relate to the desire for limiting the changes to OOLSR and Quagga.
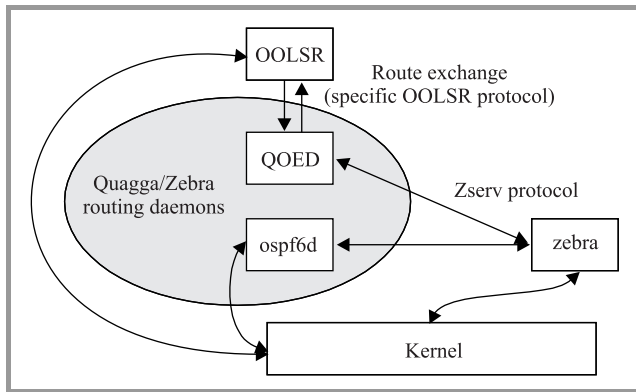

Fig. 5. Quagga/OOLSR interconnection architecture.

To Quagga main daemon *zebra, QOED* appears as a normal Quagga routing daemon, which gives some routes (OLSR routes), and asks for other routes (IPv6 OSPF routes).

To *ospf6d*, QOED appears indirectly: this daemon has the ability to redistribute routes from other protocols (such as RIP, BGP, …) QOED and OLSR appear through the routes they set in zebra.

To OOLSR, QOED appears as a daemon implementing the specific protocols for route exchanges OOLSR→QOED and QOED→OOLSR.

A crucial point of the architecture and implementation, is that, the Quagga/Zebra Zserv protocol is re-used, and also that additional protocols for route exchanges between OOLSR and QOED are used.

5. Conclusion

In this paper, we have shown how to extend OLSR in order to provide QoS support, ensure a secure routing and interconnect the OLSR and OSPF domains. All these extensions take care of MANET specificities: radio interferences, high dynamicity and low capacity resources. They have been implemented on a real MANET/OLSR platform comprising 18 nodes. Performances obtained on this platform allow us to conclude that the OLSR extensions are very useful to military applications and very significantly improve the network behavior, in particular when self-organization, mesh operations, with a possible high mobility are required. MANET solutions have to be considered today for tactical edge routing scenario, but also for transit networks, where it would require more studies concerning the scalability. MANET meets military requirements and that in particular below Brigade echelon.

References

[1] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized link state routing protocol", RFC 3626, IETF, 2003.

[2] T. Plesse, C. Adjih, P. Minet, A. Laouiti, A. Plakoo, M. Badel, P. Muhlethaler, P. Jacquet, and J. Lecomte, "OLSR performance measurement in a military mobile ad-hoc network", *Ad Hoc Netw. J.* (special issue on data communication and topology control in ad hoc networks), vol 3/5, pp. 575–588, 2005.

[3] G.-S. Ahn, A. Campbell, A. Veres, and L.-H. Sun, "SWAN: service differentiation in stateless wireless ad-hoc networks", in *Proc. INFOCOM'2002 Conf.*, New York, USA, 2002.

[4] G. Allard, L. Georgiadis, P. Jacquet, and B. Mans, "Bandwidth reservation in multihop wireless networks: complexity, heuristics and mechanisms", in *24th Int. Conf. Distr. Comp. Syst. Worksh. WWAN ICDCSW'04*, Tokyo, Japan, 2004.

[5] C. Chaudet and I. Guerin-Lassous, "BRuIT: bandwidth reservation under interferences influence", in *Eur. Wirel. Conf. EW*, Florence, Italy, 2002, pp. 466–472.

[6] K. Nahrstedt, S. Shah, and K. Chen, "Cross-layering architectures for bandwidth management in wireless networks", in *Resource Management in Wireless Networking*, M. Cardei, I. Cardei, and D. Du, Eds. Berlin: Springer, 2005, vol. 16.

[7] L. Moraru and D. Simplot-Ryl, "QoS preserving topology advertising reduction for OLSR routing protocol for mobile ad hoc networks", in *Proc. 3rd Ann. Conf. Wirel. Dem. Netw. Syst. Serv. WONS 2006*, Les Ménuires, France, 2006.

[8] Y. Ge, T. Kunz, and L. Lamont, "Quality of service routing in ad hoc networks using OLSR", in *Hawaii Int. Conf. Syst. Sci. HICSS-36*, Hawaii, USA, 2003.

[9] H. Badis and K. Al Agha, "QOLSR, QoS routing for ad hoc wireless networks using OLSR", *Eur. Trans. Telecommun.*, vol. 15, no. 4, 2005.

[10] D. Q. Nguyen and P. Minet, "QoS support and OLSR routing in a mobile ad hoc network", in *5th IEEE Int. Conf. Netw. ICN 2006*, Mauritius, 2006.

[11] D. Q. Nguyen and P. Minet, "Quality of service routing in a MANET with OLSR", *J. Univ. Comput. Sci.*, vol. 1, no. 13, March 2007.

[12] C. Adjih, T. Clausen, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing OLSR", in *Proc. Med-Hoc-Net 2003 Conf.*, Mahdia, Tunisia, 2003.

[13] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "OLSR with GPS information", in *Proc. 2004 Internet Conf.*, Tsukuba, Japan, 2004.

[14] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An advanced signature system for OLSR", in *Proc. ACM Worksh. Secur. Ad Hoc Sens. Netw. SASN'04*, Washington, USA, 2004, pp. 10–16.

[15] C. Adjih, S. Boudjit, A. Laouiti, and P. Muhlethaler, "Securing the OLSR routing protocol with or without compromised nodes in the network", INRIA RR-5747, Nov. 2005.

[16] C. Adjih, P. Muhlethaler, and D. Raffo, "Attacks against OLSR: distributed key management for security", in *Proc. 2nd OLSR Int. Worksh.*, Palaiseau, France, 2005.

[17] C. Adjih, P. Muhlethaler, and D. Raffo, "Detailed specifications of a security architecture for OLSR", INRIA RR-5893, Apr. 2006.

[18] "A border gateway protocol 4 (BGP-4)", Y. Rekhter and T. Li, Eds., RFC 1771, IETF, 1995, http://ietf.org/rfc/rfc1771.txt

[19] "Zebra ospf6d software", http://www.sfc.wide.ad.jp/~yasu/|research/ospf-v3-e.html

[20] "OOLSR", http://hipercom.inria.fr/OOLSR/

[21] "Quagga routing suite", http://www.quagga.net/

[22] "About Quagga", http://www.quagga.net/about.php

[23] K. Ishiguro, "The Zebra distributed routing software", in *North Amer. Netw. Oper. Group Meet.*, Tampa, USA, 1997, http://www.academ.com/nanog/june1997/zebra.html

Cedric Adjih is currently a researcher in the Hipercom team. He received his Ph.D. diploma in 2001 from Versailles University, France. His research interests include performance evaluation, design and implementation of mobile ad hoc networks, quality of service, queueing theory, autoconfiguration, security issues and network coding.
e-mail: cedric.adjih@inria.fr
INRIA
Rocquencourt
78153 Le Chesnay Cedex, France

Pascale Minet is vice head of the project Hipercom (high performance communication) at INRIA. She is interested in mobile ad hoc networks, wireless sensor networks, quality of service support, energy efficiency and real-time scheduling in distributed real-time systems. She belongs to the IJCIS editorial board and many international conference program committees.
e-mail: pascale.minet@inria.fr
INRIA
Rocquencourt
78153 Le Chesnay Cedex, France

Paul Muhlethaler is Research Director at INRIA. His main interests are in wireless communication systems and IP networks. He has published tens of papers in journals or internationnal conferences especially on medium access schemes, routing algorithms, performance evaluation, ad hoc networks, scheduling algorithms.

e-mail: paul.muhlethaler@inria.fr
INRIA
Rocquencourt
78153 Le Chesnay Cedex, France

Emmanuel Baccelli after working as an engineer in the Silicon Valley for Metro-Optix Inc. and as a consultant for AT&T Labs in New Jersey, USA. Became a graduate of Ecole Polytechnique, France, where he obtained a Ph.D. in computer science and mathematics in 2006. Since 2007, he is a staff researcher at INRIA, Paris. Part of the Hipercom project at Ecole Polytechnique, his focus is on ad hoc networking and its integration in the Internet, including active participation in standardization organizations such as the IETF.
e-mail: emmanuel.baccelli@inria.fr
INRIA
Rocquencourt
78153 Le Chesnay Cedex, France

Thierry Plesse received an optronics and optical telecommunications Master's degree in engineering, from ENSSAT national engineering school (Lannion, France) in 1989. He has worked with the DGA (French MoD) for 16 years, and on tactical Internet, mobile Internet, and mobile/Internet convergence projects for 10 years. He is posted in CELAR (Technical Defense Center for Information Warfare) with Bruz (Brittany, France). He received CELAR Technical Innovation First Prize in 2005 for MANET works in collaboration with INRIA.
e-mail: thierry.plesse@dga.defense.gouv.fr
DGA/CELAR
BP 7419
35174 Bruz Cedex, France