WIDENS: Advanced Wireless Ad-Hoc Networks for Public Safety

Hervé Aïache, Vania Conan,
Grégoire Guibé, Jérémie Leguay,
Christophe Le Martret
Thales Communications
92704 Colombes cedex, France
{firstname.name}@fr.thalesgroup.com

Jose Maria Barcelo, Llorenc Cerda,
Jorge Garcia
Universitat Politecnica de Catalunya
08034 Barcelona, Spain
{joseb, fllorenc, jorge, joseb}@ac.upc.es

Raymond Knopp, Navid Nikaein
Institut Eurécom
06904 Sophia Antipolis, France
{firstname.name}@eurecom.fr

Xavier Gonzalez, Audrey Zeini
EADS Telecom
78063 Saint Quentin en Yvelines, France
{firstname.name}@eads-telecom.com

Olli Apilo, Adrian Boukalov,
Jouni Karvo, Henri Koskinen,
Luca Roberto Bergonzi
Helsinki University of Technology
P.O. Box 3000, Finland
{firstname.name}@tkk.fi

Jorge Concejo Diaz
Telefonica
28043 Madrid, Spain
concejo@tid.es

Jérôme Meessen
Multitel ASBL
B 7000 Mons (Belgium)
{firstname.name}@multitel.be

Chris Blondia, Peter Decleyn,
Erwin Van de Velde, Michael Voorhaen
Universiteit Antwerpen
2020 Antwerp, Belgium
{firstname.name}@ua.ac.be

Abstract— **This paper provides an overview of the on-going European Project called *WIreless DEployable Network System* (WIDENS) which aims at defining a rapidly deployable communication system for public safety or emergency services. In this context, users expect a highly reliable communication system that can support real time applications to allow teams to collaborate in an efficient way. They also want the system to work in a spontaneous fashion and with no pre-installed infrastructures. To fit all the requirements, WIDENS takes advantage of the technology of *wireless ad hoc network*s to establish high data rate communication links on the fly. In this paper we describe the overall architecture of the WIDENS network and highlight the design of its major components.**

Index Terms— **Ad-hoc networks, Public Safety.**

I. INTRODUCTION TO THE WIDENS NETWORK

WIDENS is an on-going European Project, which aims at proposing and prototyping a new generation of interoperable Public Safety system. It designs an efficient self-organized communications infrastructure, which anticipates, targets and responds to the future needs of emergency applications and services. Placed at the intersection of Public Safety needs, of technical aspects and of economical perspectives, the challenge of WIDENS is threefold: (i) for Public Safety users: the objective is to identify the core functionalities of the system from specialists and professionals requirements for their crucial needs to respond faster and more efficiently to emergency operations, (ii) from technologies point of view: the aim is to design a scalable communication system, rapidly deployable and to validate its feasibility through a prototype and the definition of scenarios, (iii) from market interests: the goal is to propose ad hoc hotspots as access networks to existing Private Mobile Radio systems such as TETRA and Tetrapol [2].

Preliminary studies were conducted in collaboration with Public Safety professionals (fire services, police, ambulance) and resulted in the identification of the main characteristics of organizational structure, operational deployment and applications [1]. Even if detailed organizational structure varies between different Public Safety forces, they have the following common characteristics: (i) they are deployed in small groups of several units interacting among each other; (ii) they mainly follow a hierarchical structure. Furthermore, their deployment topology depends on the type and on the size of the emergency scene. Public Safety deployment scenarios fall into four groups: (i) a Concentration around a point (e.g. a bus crash); (ii) a Front line (e.g. forest fires, floods); (iii) a Ring: working around a place (not inside - e.g. urban fires, bomb deactivation); (iv) Random Distribution (e.g. an earthquake). The WIDENS network is designed to fit the organization of Public Safety forces and to provide them efficient support in all the reference scenarios.
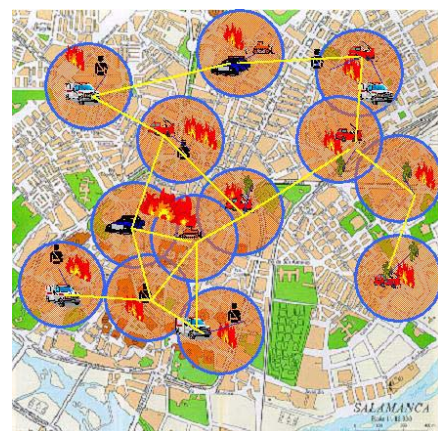

Fig. 1. Example of WIDENS Deployment Scenario.

To allow rapid deployment of the communication system, WIDENS takes advantage of the technology of Mobile Ad hoc NETworks (MANETs) [13]. An ad hoc network is composed of several mobile nodes sharing one or more wireless channels without centralized control nor an established infrastructure. All nodes communicate directly with the ones within their transmission range. Routing capabilities are added to allow multi-hop communication. Nevertheless, easy and fast deployment capabilities offered by such technology must not impair the operational efficiency of the Public Safety units with heavy network management. Public Safety teams require automated management procedures. This functionality allows them to deploy network equipment with the most appropriate pre-determined configuration to the specific reference scenario and to monitor their deployment on emergency scenes to ensure their own protection.

The delivery of high bitrate real time services like video is becoming fundamental not only for prevention procedures but also for operational interventions. Furthermore, hierarchical organizations, criticality of information exchanges and crucial nature of interventions show the necessity of communications prioritization and reliability. Thus Quality of Service (QoS), and more specifically hard QoS, mechanisms are required to respond to these requirements. QoS provisioning is a challenge in MANETs and WIDENS proposes a novel vertically integrated solution to the problem.

This paper presents first the architecture of the WIDENS system. It explains how its components have been designed to integrate hard QoS features, to control network deployment and nodes configuration, and to preserve the robustness of the network. Then the main components of the final demonstrator are described.

The overall architecture is presented in section II. Section III focalizes on the WIDENS specific design of MAC/PHY layers. Section IV describes how hard QoS is performed through a co-designed IP/MAC framework. Section V explains how security has been integrated directly within routing to reinforce system reliability. Section VI presents an overview of the final demonstrator. Section VII concludes this paper.

II. THE WIDENS SYSTEM ARCHITECTURE

First studies and requirements analysis with Public Safety Professionals showed the strong need for mobility, fast deployment capabilities, interoperability, easy upgrade of the system, as well as security and QoS features [1]. However, wireless channel variability and the frequent topology changes make the tasks of providing strong QoS guarantees, of ensuring network security and of controlling network deployment very challenging [3].

The WIDENS architecture is composed of the following (Fig. 2):
- The Enhanced 802.11 DLC/MAC/PHY Services that provide reliable communication mechanisms to support synchronized transmission and QoS. It
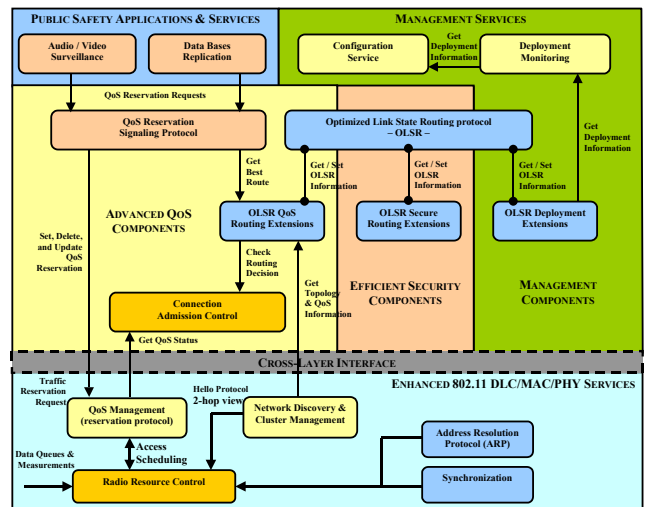

Fig. 2. The WIDENS System Architecture

cooperates with the other components through the optimized *cross layer interface*.

- The Optimized Link State Routing (OLSR) protocol is the basic routing component; this choice resulted from the analysis of mobility patterns, nodes density and traffic loads.
- The advanced QoS components of the IP layer allow a node to take local decisions for delivering IP packets through QoS routing and reservation. They are in charge of the QoS and routing signaling required for managing the dynamics of routes and associated QoS parameters.
- The Management Components support optimization of the configuration of the nodes for a given operation.
- The Security Components ensure reliability in accordance with Public Safety requirements.
- The Public Safety Applications and Services group all applications used by Public Safety units during operations.

To take into account various Public Safety users' needs, the system is designed as an extensible and modular architecture. This added flexibility would allow to anticipate the potential future evolutions of Public Safety users requirements for critical operations. The architecture of all these components and their mutual interactions are described in the following sections.

III. MAC/PHY DESIGN

A more reliable MAC layer than the commonly use of IEEE 802.11 MAC layer based on CSMA/CA is needed to support efficient ad-hoc QoS features. Inspired by the IEEE 802.11e, 3GPP, and HiperLAN/2 standard, the importance of the co-design of MAC and PHY layer with cross layering and QoS support in mind is taken into account in WIDENS. Here, we provide a brief overview of this MAC/PHY layer; more

details can be found in [4].

The network topology is organized (at the MAC layer) in 1-hop clusters as Fig. 3 shows. Cluster heads manage the radio resource within their clusters and are elected by a clustering algorithm selecting the nodes that have the maximum number of neighbors. Relay nodes are ensuring communications between clusters. Note that all nodes have the same capabilities but their roles are assigned dynamically.
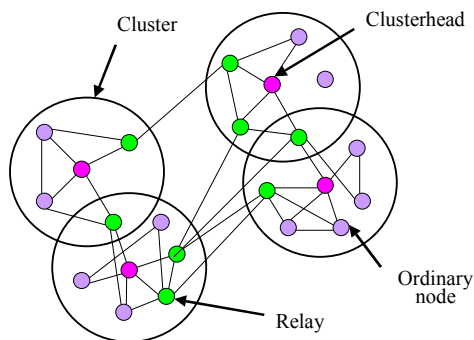

Fig. 3. Cluster Organization at MAC layer.

The WIDENS network aims at providing high bit rate wireless links using OFDM(A) modulation (802.16x proposals, 3GPP HSDPA) with high-order QAM constellations. The timing and frequency synchronization will be achieved with specially designed synchronization sequences periodically broadcasted by the cluster-head, which permit accurate simultaneous time offset estimation and carrier frequency tracking. Moreover, the signals will be designed to allow for adjacent clusters to synchronize to each other by ensuring time/frequency tracking over longer distances than those considered for transmitting data.

DLC/MAC provides advanced scheduling mechanisms based on channel state information and QoS access categories (opportunistic communication). The channel state information is obtained either by a feedback control channel or by exploiting channel reciprocity since all communication operates on a common carrier frequency per cluster. Moreover, the MAC has very fine control over physical resources and can share bandwidth between several outgoing flows in a time-varying fashion. This is crucial since nodes are capable of functioning as routers for several destinations. The DLC provides basic management services (association, bandwidth partitioning for based on QoS measures) as well as the interface with the network layer (QoS reservation mechanisms, link-quality reporting for routing, etc.). The PHY provides the basic data transport services for control plane and user plane traffic. It is based on re-configurable Orthogonal Frequency Division Multiple-Access (OFDMA) with multi-antenna capability (Multiple-Input Multiple-Output MIMO [13]). Radio-Frequency (RF) requirements are not specified since the PHY parameters (bandwidth, number of sub-carriers, etc.) can be adjusted to suit RF sub-systems depending on regional spectral regulation.

The MAC/PHY layer combines opportunistic scheduling techniques and channel coding/ARQ in a single entity. The data units are scheduled across contention and contention-free period according to QoS levels and physical resources (i.e. frequencies, antenna, time slots). This indicates that the resource allocation is done at the MAC allowing for rapid response time. The MAC/PHY layer is multi-user/stream capable (in contrast to IEEE802.11 legacy) due to time-frequency slotted nature of the channel and the OFDM(A) characteristics. Roughly speaking this architecture is an extension of the 802.11e specifications. The primary extensions are:

- Multi-user capabilities (OFDMA and spatial multiplexing).
- Mechanisms for QoS management.
- A rapid measurement feedback channel for channel states and queuing information allowing for hard-QoS support.
- Synchronization mechanisms for multi-network (multiple cluster-heads) operation.
- Enhanced link quality information in support of the network layer routing protocol.
- Tight coupling between the MAC and PHY.

IV. HARD QOS FRAMEWORK

WIDENS uses the proactive link-state routing protocol OLSR with QoS routing and a reservation protocol. OLSR is a MANET protocol [6] that provides an efficient broadcast algorithm using multi-point relays (MPR) to reduce the network overhead induced by control traffic.

QoS routing is used to find instantaneously the best routes satisfying such QoS constraints as delay or bandwidth. The route computation relies on the use of information that are spread through the network by the QoS signaling module.

The reservation scheme is used to provide strong guarantees to applications by allocating resources along routes. The decisions to admit new connections according to their required QoS guarantees and the available resources are taken by the CAC module described below. This routing layer has been designed not only to perform routing in the most efficient way regarding network resource consumption, but also to provide short response time for applications.

In order to establish the route for a new connection requiring QoS guarantees, the IP layer needs to find out a possible route that is able to accommodate the resources needed by the new connection. To do so, the following cases can occur:

- The source and the destination are in the same cluster.
- The source and the destination are in different clusters. In this case, the route can be segmented into the different Route Sections (RSs) where resources have to be allocated. These RSs can be: intra-cluster, and backbone RSs. Since each RS uses independent

resources, independent CAC must be applied to each RS.

The CAC algorithm targeted to support the reservation scheme works as follow.

Given the *Maximum Available Bandwidth* (MABi) for QoS traffic at each Mobile Node i (MNi) the following conditions have to be satisfied:

QoS constraint: $MABi \geq 0; \forall i.$ (1)

The MABi values are dimensionless and can be interpreted as the percentage of free slots available at each MNi. MABi = 0 means that no capacity is left for QoS connections at MNi. MABi < 0 would mean that the capacity that MABi is sharing has been over-reserved.
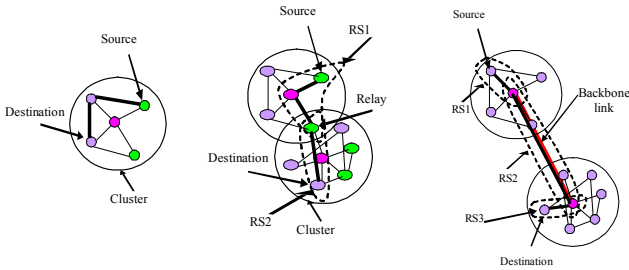
(a) Intra-cluster connection.

(b) Inter-cluster connection using intra-cluster RSs.

(c) Inter-cluster connection using a backbone RS (RS2).

Fig. 4. Cases to deal with CAC.

For each channel, the MAC layer computes and communicates to the IP layer the Maximum Available Bandwidth of the channel (MABi), and the link rate with each of its neighbors using this channel (vij). Fig. 4 shows the different types of cases that have dealt with.

In [5] we give examples of possible computations of the MABi for intra-cluster and backbone transmissions.

V. SECURED ROUTING SCHEME

Security is another key-challenge that has to be addressed in WIDENS, functions such as member or group authentication, access control, confidentiality and data integrity are strong requirements in Public Safety.

The security scheme retained in WIDENS includes features that take place at two layers:

- The network layer: As an extension of OLSR in order to provide reliability to the network by preventing malicious nodes to inject corrupted control traffic. It uses asymmetric signatures for authentication between nodes and time stamps to counter replay attacks. In the standard OLSR version nodes can come with completely wrong routing information because it can receive fake HELLO or

TC (Traffic Control) messages from an intruder in its neighborhood. A distributed Private Key Infrastructure (PKI) is used for key management.

- The application layer: Since providing security for end-to-end data communication is equivalent to that in wired networks, WIDENS takes the benefit of the PKI to ensure security between peers.

The solution proposed in [10] to provide authentication in ad-hoc networks is the basis of the WIDENS mechanism at the routing layer. WIDENS use the OLSR header defined in [10] to support securing of the routing protocol (see Fig. 5). Nevertheless, some improvements have been proposed: the implementation of a message signature with X.509v4 certificates, the usage of a certificate cache in order to minimize certificate requests and the utilization of both RSA and ECC keys.
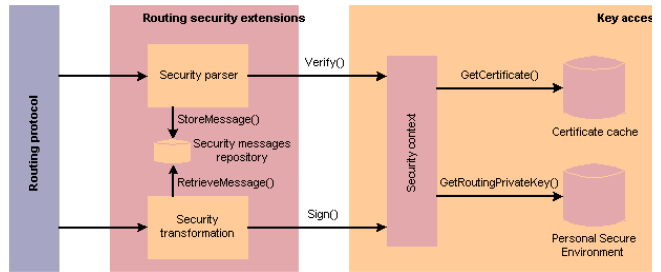

Fig. 5. Security Extensions to OLSR Components.

VI. DEMONSTRATOR OVERVIEW

The demonstration network for the WIDENS field trial will be organized into two clusters as shown in Fig. 6. The field-trial area will be around Institut Eurécom premises (France), which can be characterized as a hilly and lightly-forested terrain.

The demonstration network will consist of two clusters with one mobile node and connected at some point with both
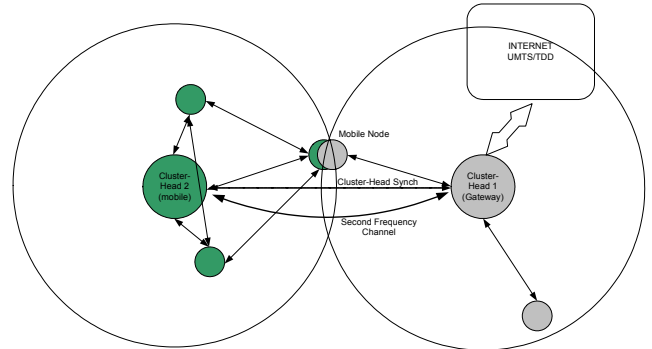

Fig. 6. WIDENS Demonstrator Elements.

cluster-heads. The two cluster-heads will be pre-configured as such. One will be fixed on the roof of Institut Eurécom and will provide gateway functionality to the internet. One node will be in proximity of the fixed cluster-head (e.g. inside the Eurécom building). The second cluster-head will be in a

specially-equipped van (220V power-supply derived from the van's engine) which can provide power for the other nodes nearby.

The objective of the demonstrator is to highlight some of the innovative techniques offered by the WIDENS radio interface and networking protocols. Specifically we will demonstrate:

- Multi-hop relaying
- High bit-rates (> 2 Mbit/s)
- Cluster-Head Synchronization
- Multi-channel operation
- Interconnection with the internet
- Limited mobility support
- MIMO signal processing

To this end, the nodes in the far-away cluster will be connected to video-sources (e.g. surveillance equipment) which can broadcast at high bit-rates to other nodes in the network. The mobile node will demonstrate the relay functionality of the WIDENS network, acting as a link between both clusters. Cluster-heads will be synchronized over-the-air at distances beyond the capacity of data transmission. This will demonstrate the mechanisms which allow for efficient QoS-aware resource management across multiple clusters (i.e. interference management).

Subject to authorization from the French frequency regulation authorities, multi-frequency operation will be
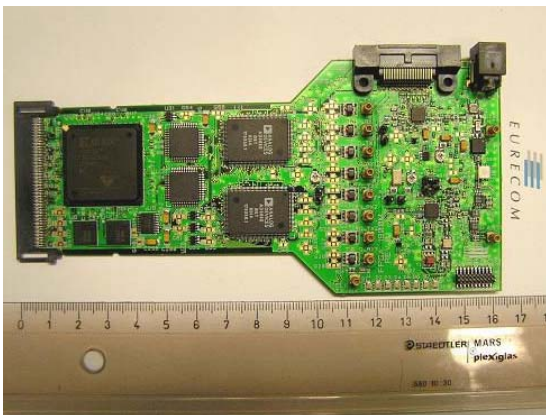

Fig. 7. Dual-Channel WIDENS PCMCIA Prototype.

demonstrated between the two cluster-heads which will setup a secondary communication channel on the second frequency. Nodes will be equipped with multi-antenna transceivers (see Fig. 7) to demonstrate the benefits of MIMO signal processing.

VII. CONCLUSION

The WIDENS project is defining a fully vertically integrated architecture based on ad hoc technologies.

This paper presented the main features of a WIDENS network, a description of the main components of the WIDENS architecture and their integration.

This architecture will be validated in the coming year through a demonstrator and simulation work. The WIDENS project thus provides an open platform for the validation of ad hoc technologies for public safety applications. The ad hoc research community will get first hand feedback from a real life prototype. The public safety technical community will be provided with a seminal testbed for further exploration of the benefits of this technology.

REFERENCES

[1] V. Conan et al., "System specifications - security, QoS, MAC, routing requirements, interfaces specifications. WIDENS, deliverable 2.2", 2004.

[2] "TErrestrial Trunked RAdio (TETRA). Web-site: www.tetramou.com".

[3] J. Macker, S. Corson, "RFC 2501: Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations", January 1999.

[4] V. Conan et al., "MAC and PHY adaptations specifications, WIDENS, deliverable 4.1", 2004.

[5] V. Conan et al., "Specification of low layer interfaces - IP/MAC mapping. WIDENS, deliverable 3.2", 2004.

[6] T. Clausen and P. Jacquet, "RFC 3626: Optimized link state routing protocol (OLSR)", October 2003.

[7] D.-S. Shiu P.J. Smith D. Gerbert, M. Shafi and A. Naguib, "From theory to practice: An overview of mimo space-time coded wireless systems", IEEE Journal On Selected Areas In Communications, 2003.

[8] S. Shenker R. Braden, D. Clark, "Integrated services in the internet architecture: an overview", in RFC 1633, June 1994.

[9] M. Mirhakkak N. Schult and D. Thomson, "A new approach for providing quality of service in dynamic network environment", 2000.

[10] Cedric Adjih, Thomas Clausen, Philippe Jacquet, Anis Laouiti, Paul Mühlethaler, Daniele Raffo, "Securing the OSLR protocol", INRIA Rocquencourt.

[11] ITU-T RECOMMENDATION X.509 | ISO/IEC 9594-8 : "Information Technology – Open Systems Interconnection – The Directory : Public-Key and Attribute Certificate Framworks", draft May 2001.

[12] MANET: Mobile Ad Hoc NETwork IETF research group: www.ietf.org/html.charters/manet-charter.html.

[13] D.-S. Shiu P.J. Smith D. Gerbert, M. Shafi and A. Naguib, "From theory to practice: An overview of mimo space-time coded wireless systems", IEEE Journal On Selected Areas In Communications, 2003.