A System Architecture for Wireless Building Automation

Wim Vandenberghe*, Benoît Latré*, Filip De Greve*, Pieter De Mil*, Steven Van den Berghe*,
Kristof Lamont*, Ingrid Moerman*, Michiel Mertens†, Jeroen Avonts †,Chris Blondia†, Guido Impens‡
*Ghent University - IBBT vzw, INTEC-IBCN, G. Crommenlaan 8 bus 201, B-9050 Gent, Belgium
†University of Antwerp - IBBT vzw, PATS, Middelheimlaan 1, B-2020 Antwerpen, Belgium
‡Telindus NV, Geldenaaksebaan 335, B-3001 Heverlee, Belgium

Abstract— Wireless Building Automation is a complex problem dealing with a lot of trade offs: on one hand sensors and actuators have to be as energy-efficient as possible, while on the other hand the overall network should be performant and resilient enough to extend or even replace a wired backbone. In addition, the network should be able to serve existing IEEE 802.11 devices such as PDAs, cameras and laptops. Furthermore, surveillance, fire detection and other critical building automation applications require end-to-end Quality of Service support to ensure the bandwidth and delay requirements also in the case of high network loads. A networking technology that simultaneously fulfills all those requirements does not exist. This paper introduces a system architecture that combines heterogeneous technologies into an appropriate networking solution.

I. INTRODUCTION

Many benefits can be gained by automating a building. Heating, ventilation, airconditioning and lighting can be controlled in a centralized and hence more optimized way, achieving extensive savings on the energy consumption and personnel cost. Entrances can be opened, locked and monitored from a single point. Surveillance cameras can be viewed and steered remotely, sensor readings can be processed centrally, and audio and video messages can be broadcasted to speakers and video screens throughout the building. It is obvious that building automation lowers the total cost of ownership, increases the security level and raises the comfort of the people inside the building.

Consequently, the building automation industry has grown remarkable the last decades, and is still going through a fast evolution. Building managers and facility managers are increasingly looking at novel technologies to lower the total installation and maintenance cost of building automation systems. Wireless technology is a key driver in reaching those goals. Indeed, installing and commissioning a myriad of wired networks has been reported to be a major source of effort and thus of cost. The multitude of wired networks in a typical professional building consists of the computer network, the fire alarm network, the emergency lighting network, the access control network, etc. Recently the different networks are being aggregated on a building automation bus system such as EIB or it's successor KNX , LON and BACNET [1]. Such a general bus replaces the different networks, diminishes the amount of necessary cables and thus decreases the cost. Replacing the wired bus for a wireless network could result in even bigger

cost savings, and could also enable new applications such as indoor positioning. It would also allow the automation of hard to reach locations and historical buildings where it is a tough job to install wires. But the deployment of such a wireless network is hindered by a number of fundamental technological problems. The IBBT WBA project [2] aims at solving those problems and at developing a solution for wireless building automation. That solution will be implemented and demonstrated in a historical building: Arts Centre Vooruit [3].

The biggest challenge we are facing is the fact that the wireless network has to fulfill contradictory requirements. On the one hand, sensors and actuators have to be as energy-efficient as possible because they are battery powered, while on the other hand the network should be performant enough to support video surveillance and extend or even replace the wired backbone. In addition, the network should be able to serve IEEE 802.11 devices and it should be scalable to support the number of devices that can be found in a large building. For instance in Arts Centre Vooruit, about 10 000 sensors and actuators and 10 cameras have to be connected [4].

A networking technology that simultaneously fulfills those requirements does not exist. Instead, heterogeneous technologies have to be combined into an appropriate networking solution. The solution proposed by the IBBT WBA project will consist of four different kinds of networks: the Wired Backbone, the Wireless Mesh Network (WMN), Wireless LANs (WLANs) and Sensor and Actuator Networks (SANETs). Figure 1 depicts this cohesion of different technologies.

The Wired Backbone will typically be a gigabit IP backbone, and can thus achieve a much higher throughput than the wireless technologies. The Building Management System (BMS) and most of the servers are directly connected to it. In some buildings it can be widely deployed, but in some cases (e.g. historical buildings), the opposite is true.

The Wireless Mesh Network (WMN) extends the Wired Backbone, connecting the WLAN and SANET to the Wired Backbone. The use of WMN routers with multiple interfaces should enable high throughputs. By means of dynamic channel selection and power control, the topology can be controlled and interference reduced. The WMN should be self-healing and self-organising, and should provide Quality of Service (QoS) by means of bandwidth reservations.

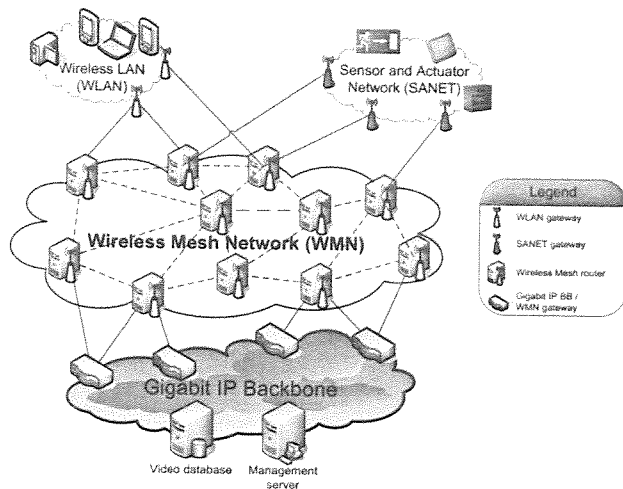The Sensor and Actuator Network (SANET) is responsible

Fig. 1. The different networks of the wireless solution

for transmitting monitor and control information with various QoS and security requirements. This involves low data rate traffic, a domain where IEEE 802.15.4 is a suitable technology. The SANET should be self-healing, self-organising, and because most wireless sensors and actuators are battery powered, the SANET nodes should consume as little energy as possible.

The Wireless LAN (WLAN) is responsible for serving IEEE 802.11 b/g devices such as surveillance cameras, PDAs, laptops, speakers and video screens. Those devices require a high bandwidth and a low latency (e.g. for video surveillance). The IEEE 802.11 access point needs to support QoS in order to allow simultaneous critical services.

Because of coverage and reliability reasons, multiple WLANs and SANETs may be connected to the WMN or Wired Backbone. Gateways are the interface points between the different networks. The functionality depends on the protocol stack that is running on these networks.

The remainder of this paper will discuss the state-of-the-art, and explain the differences between our approach and the solutions proposed in other existing projects. Section III discusses the system architecture and gives an example scenario. Finally, we conclude in section IV.

II. STATE-OF-THE-ART

A. Wirless mesh network solutions

The never ending quest to provide better service in a wireless environment has recently lead to the emergence of Wireless Mesh Networks (WMNs) [5]. In those networks, each node acts not only as a client but also as a router.

One of the most critical research challenges for such networks is to improve the capacity of the network. A multitude of techniques exists to tackle this problem [6]. We will restrict this discussion to a few examples. At the physical layer, profit can be gained using MIMO systems. At the MAC-layer, cross-layer design (e.g. MAC with power control) or the multi-channel MAC approach (where each node has multiple radios

on different channels) can boost the capacity of the network. At the routing layer, ad hoc routing protocols are not optimal for WMNs because a WMN node for building automation is not mobile. Instead, link quality source routing (LQSR) [7] and multi-radio LQSR are more appropriate protocols which use link quality metrics such as expected transmission count (ETX), per-hop RTT and WCETT [8], [9].

Although various companies start to to deploy WMN in various application scenarios, field trials show that their performance is still far below the expectations [6]. Many open research issues with respect to network capacity, scalability, self-organization, self-configuration, integration, security, etc still need to be resolved. The IEEE 802.11s task group tackles these issues and is working on a WMN standard, but a single proposol is not yet chosen, and a ratified standard can not be expected before the first half of 2008 [11].

The WMN architecture proposed in this paper supports QoS and uses a multi-channel MAC with power control for capacity improvements. Up to four radios per node will be supported. Several WMN systems are already available today, but generally one [12], [13], [14] or two radios [15], [16], [17] are used for WMN communication. Dynamic channel selection, power control and QoS support are all indispensable features of a solid WMN, but none of the existing solutions incorperates all of them.

B. Sensor and actuator network solutions

Wireless sensor networks use one-way communication between the sensors and a centralized sink which collects all the sensor's data [18], [19]. The most researched topic is to lower the energy consumption [20]. The introduction of actuators in the network however opened a whole realm of possibilities and challenges [21] such as node heterogeneity, direct communication between sensors and actuators and real-time communication. Furthermore, the increasing importance of QoS (e.g. for critical safety applications as fire detection) and security issues has raised the question for two-way communication.

Recent papers mainly focus on sensor networks and try to save energy by using different MAC-strategies, routing protocols or topology schemes. Examples include switching off the radio when no data is expected [22] or the use of an additional low power signaling radio [23]. An important conclusion is that the best way to save energy is to periodically power off the radio as the main sources of energy wastage are collisions, idle listening, overhearing and control packet overhead [24]. Little research has been done in the area of QoS. The SAR-protocol [25] creates multiple paths from each node to the sink by building multiple trees, each with its own QoS-metric. In [26] a protocol is proposed that enables real time communication in wireless sensor networks. A more elaborate overview of sensor networks and SANETs can be found in [19] and [21].

The IEEE 802.15.4-protocol has been specially designed to offer reliable and low-power communication for sensor networks, but can also be used in SANETs. The network

and application layers are defined by ZigBee [27], but do not guarantee QoS. Overall, very few papers have been published on the topic of SANETs that combine low energy consumption with QoS. In [24] an adaptive energy management scheme is proposed that controls the wake up cycle of sensors based on the experienced packet delay. Many research items still need to be tackled in the area of SANETs.

C. Wireless LAN with QoS support

The IEEE 802.11 MAC supports two medium access protocols: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). When PCF is enabled, it uses a central point coordinater to cyclically poll high-priority stations and grant them the privilige of transmitting. This way, a restricted form of QoS can be supported. However, only a few manufacturers have implemented PCF, mainly because the loose specification of PCF leaves many issues unsolved [28].

Several non-standard QoS mechanisms for IEEE 802.11 exist, and can be classified into three categories: service differentiation, admission control and bandwidth reservation, and link adaption [29]. Service differentiation is achieved by two main methods: priority and fair scheduling. Examples are Enhanced DCF (EDCF), Persistent Factor DCF (P-DCF) and Distributed Weighted Fair Queue (DWFQ). Under high traffic load conditions, service differentiation does not perform well, making admission control and bandwidth reservation necessary. Admission control schemes can be classified into measurement-based schemes such as Virtual MAC, and calculation-based schemes. Bandwidth reservation schemes generally are scheduling- and reservation-based, e.g. ARME and AACA. Finally, link adaption is desirable to maximize the throughput, since transmission rates differ with the channel conditions. Some examples are Received Signal Strength, PER prediction, MPDU-based link adaption, etc.

The recently ratified IEEE 802.11e standard aims at improving QoS support with a revised MAC layer that uses the new Hybrid Coordination Function (HCF), combining elements of both DCF (included in the Enhanced Distributed Coordination Function or EDCF) and PCF (included in the HCF Controlled Channel Access or HCCA). However, the other QoS schemes described above are left out in the IEEE 802.11e standard, although they could also improve the QoS performance [30].

III. SYSTEM ARCHITECTURE

A. Architecture overview

A possible system architecture for interworking between the wired backbone, WLAN, SANET and WMN and for wireless building automation is presented in figure 2. The architecture is broken down into three planes and three layers: the central management plane, the control plane, the data plane, the BMS layer, the network layer and the end device layer. Just like in wired infrastructured networks, we aim to separate the network into different planes. However, the management plane will be much more intelligent as it will be expanded with capacity flow management and admission control tasks, enabling a much more efficient use of the available bandwidth. In the

following part, the different building blocks of that architecture are discussed.

1) BMS - data plane: The BMS - data plane monitors data from the end devices and takes the necessary actions. It consists of different applications for the management of heating, ventilation and airconditioning (HVAC), fire detection, access control, video surveillance, tracking of persons and equipment, etc. The several actions that can be executed by these applications can be triggered manually, or automatically by various modules such as motion detection, emergency detection, etc. For high bit rate data, the BMS - data plane will request connections to the connection management with specific quality parameters such as framerate and resolution.

2) Network - data plane: This is the data plane of the different networks that were already introduced in this paper: the Wired Backbone, the WMN, the SANET and the WLAN. It forwards data from the BMS to the end devices and vice versa, using forwarding rules determined by the distributed network control.

The WMN uses IEEE 802.11a, which has 12 non-interfering channels. Maximum profit can then be gained using a multi-channel MAC with up to four radios on every node. This requires a solid channel assignment algorithm to avoid interference, which will be developped during the IBBT WBA project. Using this algorithm, the WMN nodes will set up fixed links with a selected few of their neighbours, creating a wireless switched ethernet. This will allow the introduction of known and well tested ethernet concepts in the WMN domain.

The SANET uses IEEE 802.15.4 technology for the MAC layer. ZigBee defines network and application layers on top of IEEE 802.15.4, but it doesn't support QoS and is not scalable enough for wireless building automation. Therefore, extra research is needed to solve these issues.

The WLAN could be implemented using the new IEEE 802.11e standard, or IEEE 802.11g extended with some of the QoS schemes discussed in the state-of-the-art. Research performed in the IBBT WBA project will have to determine which is the best way to go.

Three different kinds of gateways are necessary for the interconnection of these different networks: the Wired/Wireless gateway, the SANET gateway and the Wireless access point. The function of the Wired/Wireless gateway and the Wireless access point is rather straightforward: they interchange IP packets between the Wired IP Backbone, the WMN and the WLAN. No translation of packets is necessary in these gateways. In the SANET gateway however, a translation will be necessary because the SANET will not be IP based. Furthermore, the SANET gateway will act as a SANET proxy for the collection of sensor data and the network management.

3) End device - data plane: The end devices can be subdivided into two categories: low data rate devices such as sensors and actuators, and high data rate devices such as cameras, speakers and video screens. The sensors and actuators are equipped with a low-power RF module (e.g. IEEE 802.15.4), while the cameras and speakers are equipped with a high data rate RF module (e.g. IEEE 802.11). The end
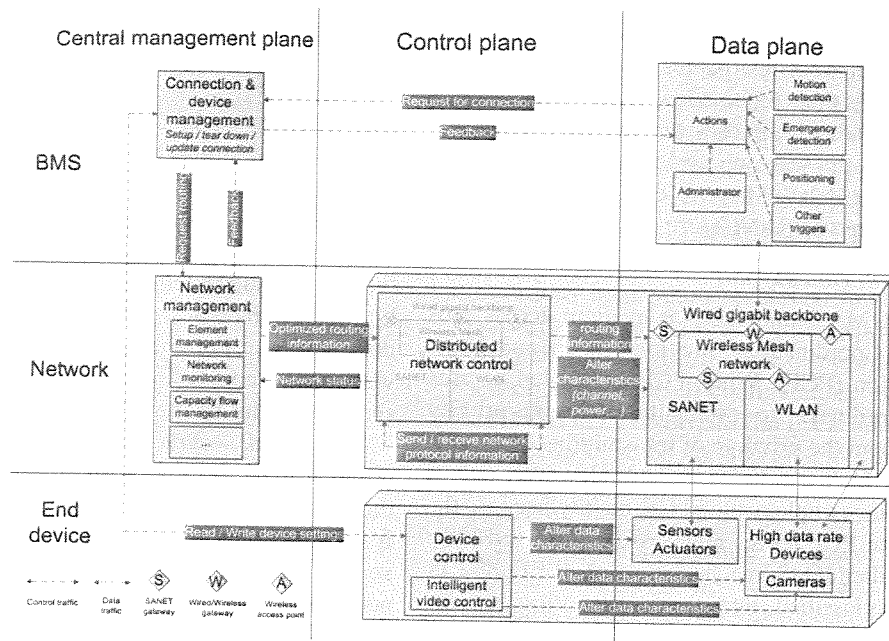
Fig. 2. Network architecture

devices generally send their data to the BMS and vice versa, but some sensors may also send data directly to one or more actuators within the SANET, e.g. when the latency introduced when going through the BMS is too high.

4) Distributed network control: The distributed network control is responsible for the set up and maintenance of the network and takes care of the self-organizing and self-healing characteristics of the network. Control information is exchanged in order to determine the forwarding rules, selected channels, transmit power, etc., which are further used by the network - data plane. Although the distributed network control tries to optimize the network with intelligent power control and dynamic channel selection, it doesn't take the end-to-end QoS demands of the different running applications into account, which is the responsibility of on the network management. The necessary information for that network management regarding spare capacity of the network is calculated using bandwidth estimation techniques such as packet pair probing. Each of the networks has its own distributed network control, and resides in each network node.

5) Device control: Each device has a built-in device control. It is responsible for the configuration of the device settings, e.g. frame rate and resolution of a camera, polling interval of a temperature sensor, sensitivity of a smoke detector, etc. Changing these settings alters the characteristics of the data streams sent over the network. Typically, the device control isn't intelligent but just executes the commands given by the device management. The Intelligent video control however changes the camera settings in an autonomous way. It can change the resolution and frame rate as a result of intelligent algorithms running on the camera (e.g. taking type of content or energy constraints into account).

6) Connection & device management: Connection and device management (CDM) aggregates the application-level requirements coming from the BMS, and translates them into reservation requests for the network management, and policy settings for the devices. By keeping a centralized view on the traffic that has to run trough the network, it can coordinate the behaviour (i.e. traffic profile) of the devices and the available capacity in the network. A policy-based delegation model will be used to implement this mechanism. Using an interative process, CDM will find an intersection between the policies (e.g. minimum and maximum bandwidth) requested by the application, the settings of the devices and the connectivity in the network.

7) Network management: In addition to the typical element management tasks such as fault, configuration, performance, security and accounting management, the network management also performs capacity flow management tasks, processing connection requests from the connection management. Using topology and network status information gathered from the distributed network control, it determines the optimal way to route the connection and interacts with the distributed network control for the optimization of the forwarding rules. This optimal route for the connection takes the already established connections into account, thus realising bandwidth reservations. For the IP networks, SNMP is a suitable network management protocol, but is not available for the SANET. Therefore the SANET gateway will act as a network management proxy, collecting and translating all SANET management information.

B. Example scenario

During the night, a burglar triggers a movement sensor in the supply room. This sensor forwards this information to

the BMS - data plane through the SANET, WMN and Wired Backbone.

In the BMS - data plane, the information from the sensor is processed and results in an action: the video of the camera in the supply room has to be shown on the monitor of the security guard. The BMS - data plane requests a connection from the camera to the screen with a high resolution and framerate to the connection management.

The connection management will then ask the network management for a connection with the bitrate necessary for the given frame rate and resolution, e.g. 4 Mbps. The network management framework, which has an up-to-date knowledge of the status of the network through interaction with the distributed network control, decides that not enough bandwidth is available and alerts the connection management, stating that only 2 Mbps is available.

The connection management then decides to reduce the bitrate using the same frame rate but a lower resolution, and requests a 2 Mbps connection. The network management calculates that it is possible to set up that connection, and takes necessary actions to optimize the routing information and QoS parameters in the network. Once this is done, the connection management is notified that the connection can be set up. The device management then configures the camera and screen with the right settings. The connection management on his turn notifies the BMS - data plane that the video stream can be started, and what the characteristics are of that video stream. Then the video stream from the camera is successfully shown on the screen of the security guard, who sees that a burglar has entered the supply room and notifies the police immediately.

IV. CONCLUSION

We have proposed a system architecture which is capable to deal with the stringent and often conflicting requirements for wireless building automation. This architecture is based on the separation of management, control and data plane and further identifies the different components and functions needed for communications over heterogeneous wireless networks with end to end QoS support. In the scope of the IBBT WBA project, remaining open security and network issues will be addressed, and a demonstrator of this architecture will be built.

REFERENCES

[1] Open Systems for Homes and Buildings: Comparing LonWorks and KNX,

[2] Wireless Building Automation,

[3] Kunstencentrum Vooruit,

[4] IBBT WBA/WP1/D1.1, "User requirements and system specification", September 2005

[5] R. Bruno, M. Conti, E. Gregori, "Mesh networks: commodity multihop ad hoc networks", IEEE Communications Magazine, Vol. 43, No. 3, March 2005, pp. 123–131

[6] Akyildiz, I.F., Xudong Wang: "A survey on wireless mesh networks", IEEE Communications Magazine, Volume 43, Issue 9, Sept. 2005, pp. 23–30

[7] R. Draves, J. Padhye, and B. Zill, "The architecture of the Link Quality Source Routing Protocol", Technical Report MSR-TR-2004-57, Microsoft Research, 2004.

[8] R. Draves, J. Padhye, and B. Zill, "Comparisons of Routing Metrics for Static Multi-Hop Wireless Networks", ACM Annual Conf. Special Interest Group on Data Communication (SIGCOMM), Aug. 2004, pp.133–44

[9] R. Draves, J. Padhye, and B. Zill, "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks", in Proc. ACM MobiCom '04, Philadelphia, PA Sept. 26Oct. 1, 2004, pp. 114–128

[10] Toumpis, S., Goldsmith, A. J., "Performance, optimization, and cross-layer design of media access protocols for wireless ad hoc networks", ICC 2003 - IEEE International Conference on Communications, May 2003 pp. 2234–2240

[11] Greg Goth, "Groups Hope to Avoid Mesh Standard Mes", IEEE Distributed Systems Online, vol. 6, no. 9, 2005

[12] SkyPilot networks, www.skypilot.com

[13] Tropos Networks, www.tropos.com

[14] Strix Systems, www.strixsystems.com

[15] Mesh Dynamics, www.meshdynamics.com

[16] The meshnode project page, www.meshnode.org

[17] A. Raniwala, T. Chiueh; "Architecture and Algorithms for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network", INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE Volume 3, Page(s):2223 – 2234

[18] Akkaya, K. and Younis,M., "A survey on routing protocols for wireless sensor networks", Elsevier Ad Hoc Networks, Vol. 3, No.3, pp. 325–349, May 2005

[19] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci,"Wireless sensor networks: a survey", Computer Networks, Volume 38, Issue 4, 15 March 2002, Pages 393–422

[20] Vivek Mhatre and Catherine Rosenberg, "Design guidelines for wireless sensor networks: communication, clustering and aggregation", Ad Hoc Networks Journal Elsevier, 2004, Vol. 2, Issue 1, pp. 45–63

[21] I. F. Akyildiz, I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges", Ad Hoc Networks Journal Elsevier, 2004, Vol. 2, Issue 1, pp. 351–367

[22] Amre El-Hoiydi and J.-D. Decotignie, "WiseMAC: An Ultra Low Power MAC Protocol for Multi-hop Wireless Sensor Networks",Proc. 1st Int. Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS 2004), Lecture Notes in Computer Science, LNCS 3121, pp. 18–31, Springer-Verlag, July 2004.

[23] C. Schurgers, V. Tsiatsis, S. Ganeriwal and M. Srivastava,"Optimizing sensor networks in the energy-latency-density space", IEEE Transactions on Mobile Computing, Vol. 1,No. 1, August 2002, pp. 70–80.

[24] A. Duressi, V. Paruchuri, L. Barolli, "Delay-energy aware routing protocol for sensor and actor networks", Proc. 11th Int. Conf. on Parallel and Distributed Systems, Volume 1, 20-22 July, 2005, pp. 292–298

[25] K. Sohrabi, J. Gao, V. Ailawadhi, G.J. Pottie, "Protocols for Self-Organisation of a Wireless Sensor Network", IEEE Personal Communication, October 2000, pp. 16–27

[26] T. He, J. A. Stankovic, C. Lu, and T. F. Abdelzaher, "SPEED: A stateless protocol for real-time communication in sensor networks", Int. Conf. on Distributed Computing Systems (ICDCS 2003), May 2003

[27] ZigBee Alliance, www.zigbee.org

[28] A. Lindgren, A. Almquist and O. Schelen, "Evaluation of Quality of Service Schemes for IEEE 802.11 Wireless LANs", Proc 26th Annual IEEE Conf. Local Comp. Nets., Tampa, FL, Nov. 2001

[29] H. Zhu, M. Li, I. Chlamtac and B. Prabhakaran, "A Survey of Quality of Service in IEEE 802.11 networks", IEEE Wireless Communications, August 2004, pp. 6–14

[30] Q. Ni, L. Romdhani, T. Turletti, "A Survey of QoS Enhancements for IEEE 802.11 Wireless LAN", Journal of Wireless Communications and Mobile Computing, Wiley, 2004, Volume 4, Issue 5, pp. 547–566

KEIO UNIVERSITY
GLOBAL COE PROGRAM

**High-Level Global Cooperation
for Leading-Edge Platform on Access Spaces**

**1st KEIO and Gent University G-COE Joint
workshop for future network 2008**

20th–21th March 2008 UGent University, Gent, Belgium