INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Team POPS

System & Networking for Portable Objects Proved to be Safe

Futurs

THEME 1A

Activity Report

2003

Table of contents

1. Team

Joint team with LIFL (CNRS and Lille University - USTL), located in Lille, created the July 1st, 2003.

Scientific leader

David Simplot-Ryl [Associate Professor, Univ. Lille 1]

Permanent Staff

Jean Carle [Associate Professor, Univ. Lille 1]
Gilles Grimaud [Associate Professor, Univ. Lille 1]
Farid Nait-Abdesselam [Associate Professor, Univ. Lille 1]

External Collaborator

Ivan Stojmenovic [Professor, Univ. Ottawa, Canada]
Jean-Jacques Vandewalle [Gemplus Researcher]

Post-doctoral Staff

Julien Cartigny [ATER, Univ. Lille 1]
Christophe Rippert [post-doc. INRIA]

PhD Students

Nadia Bel Hadj Aissa [European Contract, since January 1, 2004]
Alexandre Courbot [INRIA/Nord-Pas-de-Calais Grant, since October 1, 2003]
Damien Deville [CNRS/Gemplus/Nord-Pas-de-Calais Grant, since October 1, 2001]
Michael Hauspie [Gemplus/Nord-Pas-de-Calais Grant, since October 1, 2001]
Francois Ingelrest [Government Grant, since October 1, 2003]
Mahmoud Taifour [Syrian Government Grant, since June 1, 2002]

2. Overall Objectives

Key words: *Embedded operating system*, *exo-kernel*, *smart card*, *wireless networking*, *ad hoc networks*, *wireless sensor networks*, *mobility*, *POPS*.

The POPS research group studies solutions to improve programmability, adaptability and reachability of "POPS" (Portable Objects Proved to be Safe). The POPS family contains small and limited devices like smart cards, RFID tags (see Fig. 1) [29], wireless sensors (see Fig. 2) [27] or personal digital assistants. Such small devices are characterized by limited resources, high mobility, frequent disconnection, low-bandwidth communication, passive (no battery) or limited battery life and reduced storage capacity. Moreover, in spite of these constraints and the use in untrusted environment, users and applications require high security level for POPS. The development of applications integrating POPS suffers from lack of "*reachability*" of such platform. For instance, software development is penalized by exotic and limited operating systems. Indeed, POPS, such as smart cards, are difficult to program and high level of expertise is needed to produce software. Some efforts were taken recently with the advent of Java Cards [32], PalmOS or Windows CE. But Java Card offers a very small part of Java API and a typical application written in Java cannot be directly translated to Java Card. POPS mobility induces sudden and frequent disconnection, long roundtrip times, high bit error rates and small bandwidth. Hence, POPS systems have to adapt themselves to application requirements or modification of the environment. One can also point out that:

- First, "the POPS adjustment to the environment" reverses the current habits in which POPS are typically deployed in an environment prepared to host POPS according to the requirements imposed by the device interface such as its communication protocol.
  On the top of that, the environmental software is typically tailored to interact with POPS applications according to requirements imposed by the functionality provided by the POPS after it has been issued. Here, one part of our motivation is to focus on the adaptability of the POPS network means

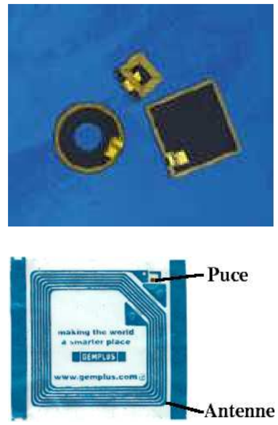

Figure 1. Example of RFID tags.

and operating system that are essential to enable POPS applications to adjust their behavior to the environment.

- Second, "the environment in which POPS find themselves operating" highlights the fact that POPS will play a key role in future infrastructures if they are generic enough to be able to discover their environment and to inter-operate with it.
  Here, the other part of our motivations is to focus on the generic nature and the maintainability of POPS network means and operating system that are essential to enable POPS devices to persist in a changing environment.

POPS research action takes advantage of its strong partnership with Gemplus since more than 14 years. This collaboration brings both partner (the RD2P research group of LIFL and Gemplus) to high level of expertise in embedded operating system design and mobile networking which are our two main research activities.

2.1.1. Embedded Operating Systems

We focus our activities on "adaptability" and on "connectivity" of embedded platforms dedicated to POPS. From then on, our researches have evolved around the smart card. In fact in the nineties (birth date of RD2P research group) smart card was the only valuable and industrially deployed POPS. Smart card integration in databases management systems, smart card integration in Corba (using the Card Object Adapter), open platform for smart card (the first smart card virtual machine), have been milestones of the RD2P research. More recently we have focused our attention (according to our industrial inputs) on embedded operating systems techniques, enabling "on-card" type checking and bytecode compression. Today smart card manufacturers and other emerging POPS manufacturers have to deal with new technological 'lock-in' inside and outside the mobile object. Dedicated operating systems are now powerful enough to run dynamically downloaded applications in a safe way. Typically Java Card loads and runs a Java-like bytecode. Nevertheless "Java-like" means "non-Java". Embedded virtual machines do not support standard abstractions. And so, Java applications cannot be deployed in a limited embedded system. On the other hand, embedded applications do not limit their needs to the Java APIs. To overcome these limitations we will focus on three complementary studies:

1. Firstly we want to study a new architectural way to embed a Java virtual machine. Conventional virtual machines are not operating systems but they overlap the abstractions proposed by the system. We plan to define a Java virtual machine designed to be the operating system (the virtual machine will manage the hardware itself).
2. Secondly, we want to define a new software infrastructure. This infrastructure aims at building of a POPS system that would only include the functionalities used to support the execution of a given set

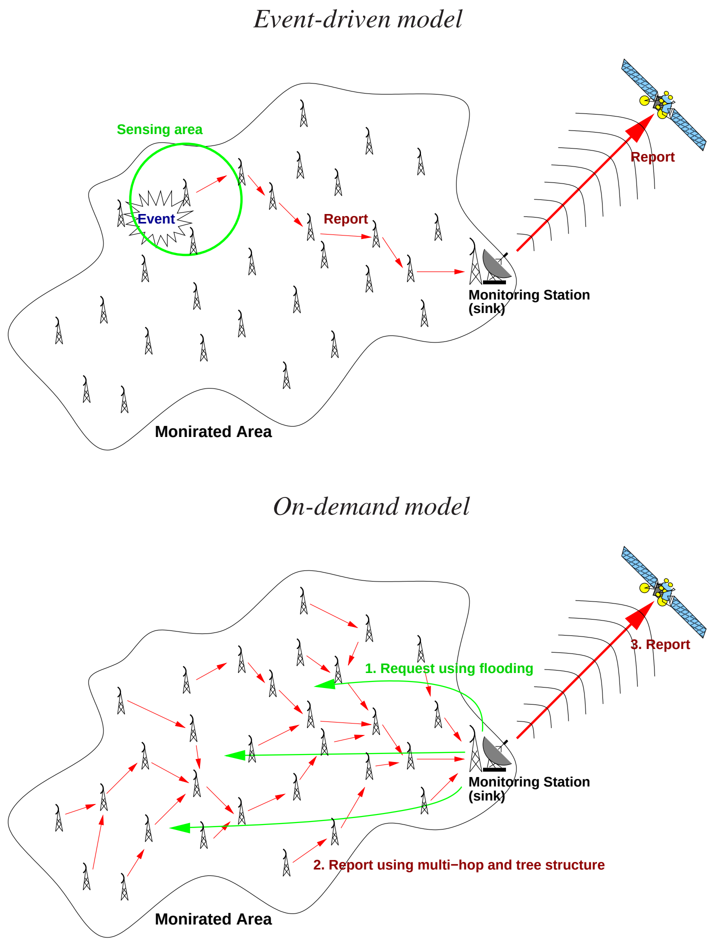

Figure 2. Example of sensor network with event-driven and on-demand models.

of applications. This JVM/OS specialisation will form the basic tools enabling a "virtually complete" version of the JVM. This action intends to increase general POPS "connectivity".

3. Java is one of the possible hardware abstractions. However different applications require different abstractions: file-system, database systems, and so on. Camille OS is a smart card Exo-kernel enabling the download of different hardware abstractions in a safe way. In this way Camille ensure POPS "adaptability" to the applications requirements. Nevertheless some critical system extensions (enhanced IO protocols for example) need additional guaranties: real-time properties and hardware resources control.

2.1.2. Mobile Networking

POPS also have a non-conventional communication interface. Due to their mobility, they have transient and unpredictable communication with other entities. This fact motivates our focussing on the ad hoc network communication model which is the most flexible model.

Indeed wireless ad hoc networks [40][36][38][31] cover a wide range of self-organized network types, including sensor, mobile ad hoc, personal area, and rooftop/mesh networks. The design of data communication techniques in multi-hop ad hoc networks has challenges at all layers of communication: physical, medium access control (MAC), network, transport and application layers. This research project concentrates on the network layer. The network layer problems can be divided into three groups: data communication, service access, and topology control problems. Data communication problems include routing, quality-of-service routing, geocasting, multicasting, and broadcasting. The protocols need to minimize the communication overhead (since bandwidth in wireless communication is typically limited) and power consumption by battery operated POPS. In service access problem, such as multi-hop wireless Internet (hybrid network, see Fig. 3), the goal is to provide or receive services from a fixed infrastructure with other hosts serving as relays if necessary. Topology control problems include neighbor discovery problem (detecting neighboring nodes located within transmission radius) and network organization problem (deciding what communication links to establish with neighboring nodes, sleeping period operations and adjusting transmission radii). Secure routing faces the following challenges: node selfishness, threats using modification of routing information, misrepresenting identity, fabrication of routing messages by one node, or between two malicious nodes (wormhole attack), and self-organized public-key management and authentication services. The main paradigm shift is to apply localized (or greedy) schemes as opposed to existing protocols requiring global information. Localized algorithms are distributed algorithms where simple local node behavior achieves a desired global objective. Localized protocols provide scalable solutions, that is, solutions for wireless networks with an arbitrary number of nodes, which is one of the main goals of this research project.

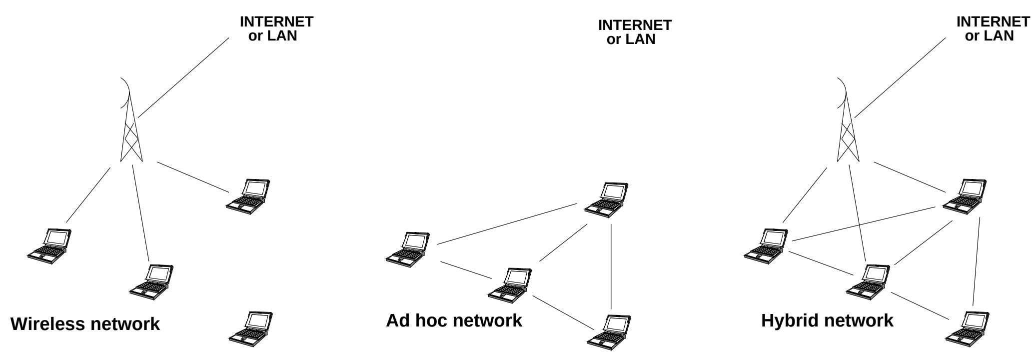

Figure 3. From wireless network to hybrid networks.

3. Scientific Foundations

Key words: *Embedded operating system*, *exo-kernel*, *smart card*, *wireless networking*, *ad hoc networks*, *wireless sensor networks*, *mobility*, *POPS*.

The POPS research group investigates solutions to enhance programmability, adaptability and reachability of small objects designated as "POPS" (Portable Objects Proved to be Safe). The POPS set includes small devices like smart cards, RFID tags or personal digital assistant which are characterized by limited resources, high mobility and high security level in spite of untrusted environment. The development of applications integrating POPS suffers from lack of "*reachability*" of these platforms. Indeed, most POPS are not easy to program and high level of expertise is needed to produce software for such limited operating systems and devices. Moreover, POPS mobility induces sudden and frequent disconnections, long roundtrip times, high bit error rates and small bandwidth. Hence, POPS systems have to adapt themselves to applications requirements or modifications of their environment. In this context, we are conducting research in the two following connected areas:

- **Embedded Operating Systems**, focusing on operating systems and virtual machines scalability (in terms of memory, microchip performance and energy) where smart cards are our reference target. Our main activities deal with the scalability of Java abstractions (the "Java in the Small" sub-project) and efficient, extensible and safe hardware management (the "Camille NG" sub-project).
- **Mobile Networking**, focusing on communication protocols on wireless network architectures, in ad hoc or wireless LAN mode, using or not fixed infrastructure. Our protocols aim to ensure secure connectivity and QoS enhancement of dense large networks which are constituted of small devices with high mobility.

POPS software architecture has never stopped evolving. Since birth of smart cards (for instance) in the early eighties, we can distinguish four different generations of software architectures, from the rough, monolithic "smart card mask" to the ultra light "post-issuance" open kernel. Nevertheless, all software generations are still used today. A rough monolithic smart card OS is the only way (known by the industry) to product low-end/low-cost smart cards. "Post-issuance OS" like Java Card are sold for the high-end market.

The smart card example has shown that embedded software is a huge family. In fact, according to the limited capabilities provided by the hardware, an embedded application offers "limited" functionality. Nevertheless the omnipresence of the POPS (over 10^9 smart card around the world today) implies a great diversity of software. And the Subscriber Identification Module (SIM) inserted in our GSM, is very different from sensors used in wireless sensor networks. All of them are supported by a powerless hardware with limited resources (memory, CPU and energy). They all suppose the use of dedicated APIs and tools. They are built over dedicated underlying operating systems...

Supporting at the same time the whole set of abstractions used by each possible embedded application is obviously impossible. To overcome this technological lock our research group has proposed to embed the use of Exo-Kernel architecture [28]. Exo-kernel architecture consists in suppressing any abstraction consideration in the (Operating System) kernel design.

Basically if we consider the conception of a conventional file system, we can define three internal layers (see Fig. 4). In a conventional "monolithic OS" The bottom layer manages the hardware, allocating sectors, or flash memory pages, programming the burn of data, etc...The second layer implements basic software to simulate a virtual device easier to administrate and to use: "the file system". The top layer manages the software security by controlling the files access. In a μ-kernel, the 'kernel' of the operating system does not support a preferred abstraction but only manage (in a preferred way) the hardware and offer a safe and secure access for different abstractions implementations. In this way, μ-kernels allows the coexistence of multiple hardware abstractions. But recent results contest the performances of such OS architectures. In an operating system the performances of provided abstractions are greatly improved when they are correlated to the adequate hardware management. That's why Exo-Kernels architects claim that "the exo-kernel must offer a safe hardware exposition without any abstraction". Software applications must be able to access the hardware and manage it according to their own goals. It is the best way to ensure dynamic adaptability to the applications requirement.

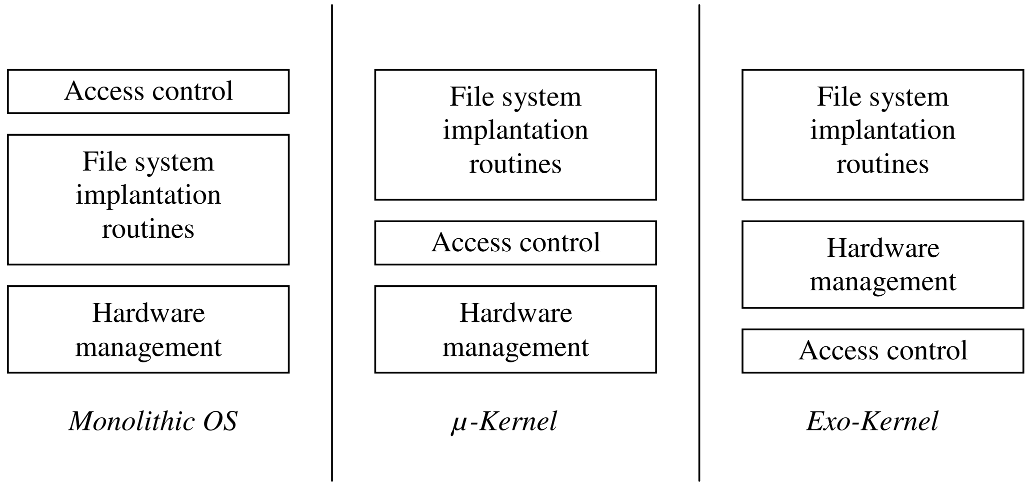

Figure 4. From monolithic OS to exo-kernel architecture.

We have proved the feasibility of this kind of kernel in a tiny device. However, it is an incomplete purpose because some hot OS topics can be loaded in a safe way. Safety is ensured statically, while the OS component is loaded. The Kernel Trusted Computing Base uses the "Proof Caring Code" principles [34]. Nevertheless, the current Camille OS defines security in terms of confidentiality and integrity, not in term of availability. Problems are related to Real Time software and Resource Control. These goals are one of our next actions called Camille NG.

Smart card is probably one of the most limited devices in the POPS family. Important industrial efforts were made to invite Java developers to deploy Java software on cards. Nevertheless tiny operating systems like Java Card OS does not really satisfy Java developers. In this way, our work around Camille (supporting dynamic extensions of the embedded OS) looks insufficient. In fact Camille enables multiple hardware abstractions justified by multiples applications needs. However, real powerful abstractions, like those proposed by Java technologies, were clearly not deployed in POPS. To invite conventional software designer to deploy they work on POPS we propose to study new OS approach to deploy Java In The Small.

POPS also have non-conventional communication interfaces. Due to their mobility, they have transient and unpredictable communication with other entities. This fact motivates us to focus on the ad hoc network communication model which is the most flexible model.

The most suitable kind of network for POPS are wireless ad hoc networks which cover a wide range of self-organized network types. Ad hoc networks are multi-hop networks consisting of wireless autonomous hosts, where each host may serve as a router to assist traffic from other nodes. Wireless ad hoc networks cover a wide range of network scenarios, including sensor, mobile ad hoc, personal area, and rooftop/mesh networks. Sensors provide service to monitoring stations. Mobile ad hoc networks are pure infrastructure-less networks used in disaster relieves, conferences, hospitals, campus and battlefield environments, with laptops, palmtops, cellular phones or other devices serving as nodes. Rooftop/mesh networks provide high-speed wireless Internet access to homes and offices.

Nodes (hosts) in an ad hoc network can be static or mobile, and can switch between active and sleeping modes. The control is distributed, thus each POPS makes independent decisions following a common pre-established protocol. An ad hoc network may be linked to a fixed infrastructure (to receive or provide service) or can function on its own. Wireless networks of sensors are likely to be widely deployed in the near future because they greatly extend our ability to monitor and control the physical environment from remote locations and improve our accuracy of information obtained via collaboration among sensor nodes and online information processing at those nodes. Networking these sensors will revolutionize information gathering and processing in many situations (*e.g.* monitoring and reporting fires, chemicals, intruders etc.). Home or office appliances can be networked in a personal area network, with input from a fixed station or mobile human. Rooftop networks are static networks with nodes placed on top of buildings. They are applied in the mesh-networking approach, where the neighborhood is 'seeded' by the installation of a 'neighborhood access point' (NAP), a radio base-station connected to the Internet via a high-speed connection. Homes and offices within range of this NAP install antennas of their own, enabling them to access the Internet at high speed. Each of these homes and offices can also act as a relay for other homes and offices beyond the range of the original NAP. As the mesh grows, each node communicates only with its neighbors, which pass Internet traffic back and forth from the NAP. It is thus possible to cover large area quickly and cheaply. For providing fixed-wireless access, the mesh approach is technically superior to the traditional 'point-to-multipoint' radio approach. It requires much less power, offers multiple paths for choosing the quickest route, is robust and scales up easily. Ad hoc networks will make communications technology useful for people everywhere regardless of nature and availability of backbone infrastructure.

In a crowded environment, such as sport arena, phones could pass traffic from other phones to base stations in adjacent cells, thus boosting capacity. Reduced power also reduces the interferences when a call is multi-hopped to the same base station instead of being directly transmitted. Calls between users within the arena could be handled locally, without loading the cellular network.

Commercial developments of wireless networks have been so far basically limited to the single hop scenarios, with one link between a mobile node and the fixed infrastructure (*e.g.* cellular telephony), or between two mobile/wireless nodes (*e.g.* Bluetooth short range technology). Single-hop wireless networks already pose significant challenges due to limited bandwidth and battery power restrictions. Multi-hop wireless networks can be modeled as a graph, with two nodes joined by an edge if and only if they are able to directly communicate with each other. The most popular model in literature is the model of a unit graph. In a unit graph, a message sent by any node reaches simultaneously all its neighbors whose distance to the transmitting node is no more than the transmission radius, which is equal for all nodes. Variations of the model includes adding obstacles, having different transmission radii for each node, or introducing minimum and maximum transmission radii, where nodes closer than minimum radius receive message, farther than maximum radius, do not receive message, and uncertain reception in between the two radii.

The selections of best data communication protocols at the network layer are certainly affected by developments, current and future, on other layers below and above the network layer. For instance, the physical layer decides whether omni directional or directional antennas are used. If antennas are omni directional, which is a typical assumption, then a message sent by one node can be simultaneously received by all its neighbors (so called one-to-all model). Some recent developments exploit the use of directional 'smart' antennas, fixed narrow beam (reaching only one neighbor, one-to-one model), wide fixed beam, or variable angular size beam antennas (one-to-many models). The ultra-wideband (UWB) transmission involves transmitting very short pulses on a wide range of frequencies simultaneously at low power. Such pulses, less than billionth of a second long, pass unnoticed by conventional radio receivers, but can be detected by a UWB receiver. Information is encoded into streams of pulses, millions of which can be sent every second, by varying their polarity or their timing relative to an apparently random but pre-arranged schedule. UWB received a massive boost in February 2002, when it received limited approval for transmissions up to about ten meters. UWB is capable of data rate of over 100 megabits per second on such short distances. Work is well advanced on the standard to enable UWB devices to locate and communicate with each other. Ad hoc networking is expected to receive further boost after adopting UWB transmission. Infrastructure-less, ad hoc UWB networks are also called 5G.

The current 'popular' choices, or dilemmas, at the medium access control (MAC) layer is between IEEE 802.11 where all POPS communicate on the same channel, and the Bluetooth that uses frequency hopping and master-slave relations. The design of medium access layer for UWB transmission is under way. UWB supports existing 802.11, 802.15.3 and HiperLan MAC standards but they do not exploit position-aware information enabled by UWB.

The research on wireless ad hoc, sensor and local area networks is booming recently within both computer science and electrical engineering communities. Both ACM and IEEE organize symposia exclusively dedicated to ad hoc networks, now in the second and third years of existence. This is in addition to increasing number of papers on ad hoc networks at main events such as IEEE INFOCOM, ACM MOBICOM, IEEE ICC, IEEE Int. Symp. on Computers and Communications, IEEE Parallel and Distributed Symposium, and IEEE Int. Conf. Distributed Computing. Despite of the enormous interest in ad hoc networks (due to upcoming commercial applications), satisfactory solutions for some fundamental problems in their operation, such as routing, broadcasting, multicasting, and network organization, are still not found.

4. Application Domains

Key words: *Telecommunication*, *ambient computing*, *banking application*, *military area*, *environment*.

Application domain of our research activities is very wide since it concerns domains commonly addressed by smart object issues:

- individual authentication in information systems, like in banking system (bank smartcards), mobile phone system (SIM cards) or wireless networking (smartcard for Wi-Fi),
- adaptable and robust networking, like in infrastructure less communication system (military communication system or emergency communication system),
- ambient computing which uses intensively POPS,
- environment surveillance systems which can use wireless sensor networks.

5. Software

5.1. Java In The Small

Key words: *Java-OS*, *embedded system*.

Participants: Alexandre Courbot [Corresponding author], Gilles Grimaud, Christophe Rippert.

Java's initial goal was to allow high level software development on small devices. Eventually it found success and promotion with software deployment on the Web, and more recently as a solution for huge enterprise servers and massive parallel computing. Today small targets are still supported, but with dedicated (Java-like) APIs and VMs. These specific technologies dramatically restrains the context in which Java applications can be deployed.

JITS focuses on these technologies and on enhancements to allow the use of a real Java Runtime Environment and a Java Virtual Machine everywhere by targeting tiny devices such as SmartCards. These devices usually doesn't use a Virtual Machine layer over an OS, but expect the Virtual Machine to be the OS. This is possible thanks to the JVM features which can be presented as a specific hardware abstraction for most of them.

JITS platform can be found at the URI http://www.lifl.fr/RD2P/JITS.

5.2. CAMILLE NG

Key words: *Exo-kernel*, *embedded system*, *real-time*, *extensibility*.

Participants: Nadia Hel Hadj Aissa, Damien Deville [Corresponding author], Gilles Grimaud.

The Camille operating system (a dedicated exo-kernel) aims at supporting the various hardware resources used in smart cards, without specializing abstractions. The architecture principle is very similar to the MIT Exo-Kernel principles and concepts. The Camille OS provides the following three basic characteristics. Portability is inherited from the use of an intermediate code and by a limited set of hardware primitives. Security is ensured by a code-safety checking (which uses a PCC-like algorithm) at loading time. Extensibility is provided through a simple representation of the hardware that at the root of the system does not predefine any abstraction. Thus, applications have to build or import abstractions which match their requirements. The Camille splitted architecture is described Fig. 5.

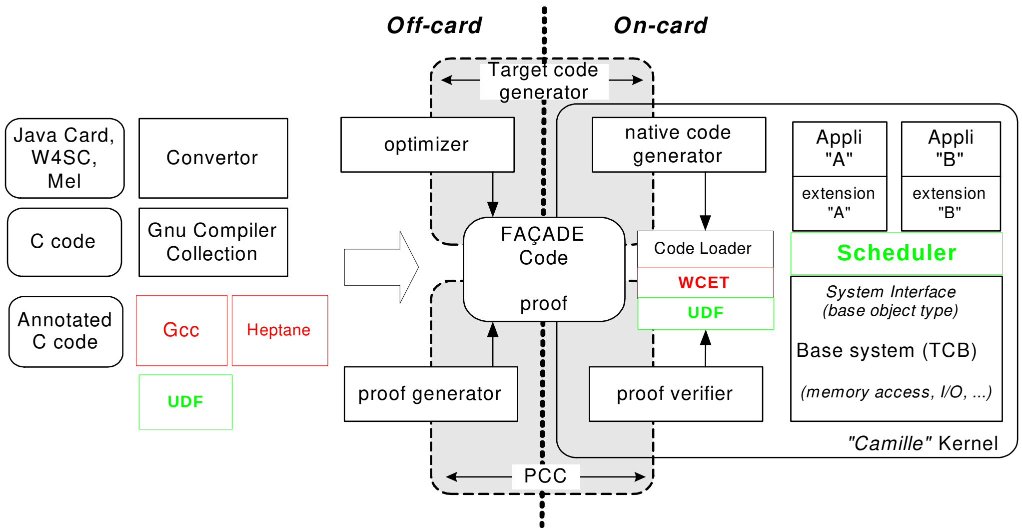

Figure 5.

The usual downside of extensibility is performance. For some parts of the OS that require efficiency, Camille uses Just-in-Time techniques to compile intermediate code into native one. Increased performance also comes from the exo-kernel approach that does not introduce abstraction penalties in the core of the OS. Because smart cards have limited computing power, additional hardware independent optimizations are also performed out of the card, while the source code is translated to FACADE. A more precise description of Camille, and experimental results as well can be found in [6]. The Camille prototype demonstrates the feasibility of an extensible smart card OS that has reasonable footprint: 17 KB of native code in which 3.5 KB for code verification, 8.5 KB for native code generation, and the rest for hardware multiplexing.

CAMILLE NG platform can be found at the URI http://www.lifl.fr/RD2P/CAMILLE.

5.3. SimTag: a simulator for anti-collision protocol design for RFID Tags

Key words: *RFID tags*, *anti-collision*.

Participant: David Simplot-Ryl.

SimTag is a simulator dedicated to anti-collision protocols. It includes protocols from ISO-18000-3 standard [30] and allows to test numerous parameters. It has been used by engineers from Gemplus and TagSys to tune their own protocols that are now included in standards.

SimTag can be found at the URI http://www.lifl.fr/RD2P/simtag.

6. New Results

6.1. Next Generation of POPS Operating System Design

Key words: *Embedded systems*, *Extensibility*, *Real Time*.

Participants: Damien Deville, Gilles Grimaud.

Emerging technologies challenges the present and futures issues in smart card (and others POPS) operating system design. In this context, the recent POPS teams research firstly focus on definition of a new smartcard vision. “Now, smart cards lack some important features which make them too far from what they should be: extensible, reactive, available, and efficient.” [6][18]. According to this vision shared by the Roadmap for European research on Smartcard Technologies and the current Inspired Integrated Platform, our recent works and first results [17] promote Real Time features scaled to POPS targets. Nevertheless Real Time principles and Exo-Kernel extensibility (claimed by our first works) introduce new scientific locks and needs additional studies.

6.2. Compiling in the Very Small

Key words: *Compilation framework*, *Embedded compilation*, *Intermediate languages*.

Participants: Damien Deville, Gilles Grimaud.

The efficiency also claimed by our vision supposes the definition on a new code management [19]. Nevertheless POPS are well known for being low end platforms with limited resources and computing power. Thus they are not provided with embedded compilers which are said to be expensive and prefer using byte code interpreters rather than just in time compilers. Our last scientific results challenge this idea and motivate the expected benefits of an embedded on the fly compilation process. Tracks are given to succeed in compiling in the very small. Some first architectural and experimental results are extracted from the Camille generic embedded on the fly code compiler.

6.3. Introducing Research Issues for Next Generation Java-based Smart Card Platforms

Key words: *Java-OS*, *JavaCard*, *Embedded Java*.

Participants: Alexandre Courbot, Gilles Grimaud.

The vision challenges next generation Java-based smart card platforms [8]. Betting on a continuous evolution towards open computing devices, next generation cards will consist in embedded Java micro-server platforms. Those platforms will be able to serve various types of services and applications thanks to two important system features: adaptability and maintainability. Two features that will have to be carefully implemented in the research agenda’s topics: real Java for cards, cards integration in a networked world, and flexible and adaptable. This research activity is well understood and supported by our industrial partner Gemplus.

6.4. IEEE 802.11 MAC Enhancements for Fairness Improvement in Wireless Ad-Hoc Networks

Key words: *wireless ad hoc networks*, *routing*, *fairness*, *QoS*.

Participants: Farid Nait-Abdesselam, Mahmoud Taifour.

Because ad-hoc networks deploy multi-hop routing protocols, where each node, in addition to its own packets, has to forward packets belonging to other nodes, selfish behavior may represent a significant advantage for a node, saving his battery power and reserving more bandwidth for its own traffic. However, if a large number of nodes start to behave non cooperatively, the network may break down completely, depriving all users from communicating. To avoid misbehavior of the mobile nodes in wireless ad-hoc networks, compensation has to be made in order to encourage all the nodes in routing other nodes’ packets without any degradation of their own data transmission.

While there has been a lot of research work on improving fairness in the presence of hidden terminals or high load of congestion, to the best of our knowledge there is no research work focusing on the differentiation between the own and routed data traffic to achieve fairness improvement. In our previous work [23][22], we have designed a routing-aware adaptive MAC (RAMAC) for IEEE 802.11 technology, which uses a routing based backoff algorithm instead of the legacy binary exponential backoff, to take into account the routing role of a given node. This new mechanism has showed all its effectiveness in the presence of nodes participating in routing and other nodes which are only using the routing service of intermediate nodes. However, the proposed RAMAC mechanism favors too much the routing nodes in comparison to the non routing nodes. In order to minimize this problem, we introduced enhancements to RAMAC by (1) differentiating between routed and own packets on top of the MAC layer, and (2) by smoothing the multiplicative factor involved in the computation of the new contention window value, in order to reach a better fairness in sharing the bandwidth [10].

6.5. Energy-efficient localized broadcast protocols for wireless ad hoc networks

Key words: *Wireless ad hoc networks*, *broadcasting*, *energy efficient protocols*.

Participants: Julien Cartigny, Francois Ingelrest, David Simplot-Ryl.

Broadcasting is an important task in wireless ad hoc networks. Since this functionality is intensively used, it is necessary to reduce the energy cost of a broadcast since POPS are energy limited. We have proposed several significant localized improvements of well-known Neighbor Elimination Scheme (NES) [35][39]. A localized algorithm is a algorithm which requires only local information in opposition to globalized algorithms which need the knowledge of entire network. Hence, we have provided a speed-up variants of NES [14][16] which reduce the inherent latency of the protocol. This protocol performances, in term of energy consumption, can be compared to MPR performances [37].

The second improvement is the reduction of supervised neighbor set to RNG neighbors or LMST neighbors [41][33]. These sets are sufficient to guarantee the coverage of the network and the system is more robust (against mobility or error transmissions) than with complete neighborhood. This improvement published in [3] is also shown more robust than MPR protocol.

The other improvements concerns the adjustment of transmission range to non-covered RNG or LMST neighbors [5][4][26] and the use of directional antennas [24]. These protocols compete with the well-known globalized broadcast protocol with range adjustment BIP [42].

6.6. Area Coverage and Energy-Efficient Protocols for Wireless Sensor Networks

Key words: *Area monitoring*, *activity scheduling*, *data aggregation*, *wireless sensor networks*.

Participants: Jean Carle, David Simplot-Ryl.

We consider area monitoring problem with wireless sensor networks. Typical applications are regular reports such as temperature monitoring or events (e.g. fire, intrusion) reporting [27]. Sensors that are energy limited devices have to self-organize themselves in order to monitor the target area as long as possible. We propose to split this problem into three separate subproblems and to consider solutions with fixed or variable transmission radii. The first one is the area coverage algorithm that aims to reduce the number of sensors needed to monitor the area (all sensors are assumed to cover circular area of equal size). The protocol allows to switch off some sensors and to periodically change the set of covering sensors in order to extend network life. The second problem is the request propagation from the monitoring station to the covering sensors which should be done in energy-efficient manner. This is known as the broadcasting task which can be solved in localized manner, by applying dominating sets (in case of fixed transmission radii) or localized minimum spanning trees (in case of variable transmission radii). The third and last problem address aggregation of sensor replies from sensors to the monitoring station. This is done by following the constructed broadcast tree in reverse order with possible fusion of data. An overview of these techniques is given in [13] and technical papers are in preparation.

6.7. Partition Detection and Replication Decision Algorithm

Key words: *Mobile wireless ad hoc networks*, *partition detection*, *replication*.

Participants: Jean Carle, Michael Hauspie, David Simplot-Ryl.

In this part, we give tools to help nodes to predict partition detection between two nodes connected via multihop route. Several metrics using network topology have been proposed [21] and an implementation of the most efficient measure has been proposed [20]. This metric allows predicting 80% of partitioning that permits to engage replication algorithms of indispensable data or services.

7. Contracts and Grants with Industry

7.1. Gemplus partnership

Participants: Alexandre Courbot, Damien Deville, Gilles Grimaud, Michael Hauspie, David Simplot-Ryl [Scientific responsible], Jean-Jacques Vandewalle.

Since its creation RD2P has been supported by Gemplus within the framework of a partnership agreement that lasts since 14 years. Gemplus has been continuously supported the RD2P research activities though fundings and the sharing of experiences and problems between RD2P and Gemplus Labs researchers.

RD2P has been a provider of innovative technologies for Gemplus thanks to several major patents (including those for a secure interpreter, a database card, a loader-linker of code, or communication protocols for tags), and thanks to thesis and projects such as: the card interpreter CAVIMA (1991), the "blank card" model (1991 and 1995), the CQL card and its integration in ODBC (from 1991 to 1994), a 32-bit RISC architecture for smart cards (1996), a programmable open card and its integration in object-oriented systems (1996), the language for the GemXplore 98 cards (1997), the integration of smart cards in transactional systems (1999), optimized communication protocols for tags (from 1999 to 2001 with Gemplus Tags), the card system CAMILLE (2000), or the card with multiple execution contexts.

Gemplus and RD2P have also gained benefits from this partnership through National or European projects in which they participate altogether: CASCADE (IST 4th framework), CESURE (RNRT), COMPiTV (RNTL), RESET (IST 5th framework), and INSPIRED (IST 6th framework).

At that present time, their partnership is mainly focused on embedded operating system research activities (JITS, Camille, and OS customization) and is strengthened by the presence of a Gemplus researcher (Jean-Jacques Vandewalle) within the RD2P research group.

7.2. TagSys partnership

Participant: David Simplot-Ryl.

In fact, TagSys is the old RFID department of Gemplus. TagSys is a spin-off company of Gemplus. The result of TagSys and RD2P partnership was the ISO 18000-3 standard about anti-collision protocols for 13,56 MHz RFID tags. This protocol is the best known anti-collision protocol and can reach a rate of 250 tags per second while other standards only provide 50 tags per second. At that present time, the partnership concerns anti-collision protocol improvements with smaller devices (in term of silicium surface).

7.3. IST-2002-507894 INSPIRED "Integrated Secure Platform for Interactive Personal Devices" (IP)

Participants: Nadia Bel Hadj Aissa, Gilles Grimaud, David Simplot-Ryl [INRIA representative].

More than other IT domains, the smart card industry is facing the challenge to reinvent itself in the fast moving high-tech area where seamless connection, mobility and security are key aspects. This breakthrough is only possible by changing the fundamentals of the smart card and by creating a new and open technology platform.

The smart card has been successful in providing a first generation of secure, personalized and portable device to millions of users principally in off-line applications such as bank and telecom. INSPIRED will develop the second generation called Trusted Personal Device (TPD) to provide Trust and Security to users and on-line services in the future ambient intelligence and ubiquitous computing environments.

The concept of an individual object representing the root of trust is the paradigm which definitely made the success of the smart card. INSPIRED intends to rely and it and to extend it for the next generation of secure communicating devices.

These devices will have different form factors and features depending of the targeted applications. INSPIRED aims at defining the common technical foundations to allow cost-efficient product developments of devices with extended features and performances that can better be integrated in heterogeneous networks.

The INSPIRED consortium gathers the large majority of the stakeholders in the European smart card arena including the major smart card manufacturers, vendors of chips and sensors for smart cards and leading research institutes. The consortium also includes companies representing users from dynamic market segments such as telecom, electronic ID, on-line services and digital rights management for requirements and concept definition and the validation of the project results.

INSPIRED is in-line with the RTD requirements identified by the RESET roadmap and will deliver the industry standard architectures for next generation devices that will overcome current technology heterogeneity and limitations.

List of participants: Gemplus (France), Schlumberger (France), Giesecke & Devrient (Germany), Oberthur Card Systems (France), Orga (Germany), Philips Semiconductors (Germany), Orange (France), Universidad Rovira i Virgili (Spain), Atmel (France), University of Twente (Netherlands), INRIA (France), Universite Catholiques de Louvain (Belgium), Infineon (Germany), NDS (Israel), Activcard (France) and Everbee (France).

8. Other Grants and Activities

8.1. National Actions

8.1.1. AS "Nomadicité des utilisateurs et adaptation dynamique de systèmes informatiques à dominante logicielle" (2002-2003)

Participants: Julien Cartigny, Michael Hauspie, David Simplot-Ryl.

Computer users often make use of several environments such as desktop and laptop computer at office, home, PDA or phone environments. Moreover, the capacity of connectivity to the network is growing. It is natural that users require more and more to have interoperability between this virtual environments which can be acceded by various and heterogeneous devices. This research action aims to develop solutions which allow taking benefits of new generation of networking, in particular to permit the connectivity continuity in mobility with wireless link (such as Wi-Fi).

List of participants: LIFL Univ. Lille 1 GOAL (C. Gransart) and RD2P (D. Simplot-Ryl) research groups, I3S Univ. Nice, Mainline (P. Sander) and Rainbow (M. Riveil) research groups, IRISA Armor project (F. André), LIP6 (B. Folliot), LSR-IMAG-INRIA Grenoble SARDES project (D. Hagimont)

8.1.2. AS "Méthodes et outils pour le développement de systèmes d'exploitation" (2002-2003)

Participants: Damien Deville, Gilles Grimaud.

List of participants: EMN (G. Müller), LIP6 Univ. Paris 6 (B. Folliot), IRISA (I. Puaut), LIFL Univ. Lille 1 (G. Grimaud), INRIA Rhône-Alpes (D. Hagimont).

8.1.3. ACI Objets Mobiles Communicants (2001-2003)

Participants: Jean Carle, Julien Cartigny, David Simplot-Ryl.

The Communicating Mobile Objects (CMO) project is studying software dedicated to interconnection and interaction for mobile objects from the real world. In a near future, a lot of mobile objects from the real world will include electronic chips. These chips will be associated with communicating devices so that cooperation between objects will be realistic. The development of such architecture requires dedicated middleware which do not exist today and improvement of networking capabilities in mobile environment.

List of participants: LIFL Univ. Lille 1, GOAL (C. Gransart) and RD2P (D. Simplot-Ryl) research groups.

8.1.4. ACI Sécurité Informatique SPOPS "Système pour POPS" (2003-2005)

Participants: Damien Deville, Gilles Grimaud, David Simplot-Ryl.

List of participants: LIFL Univ. Lille 1 RD2P (G. Grimaud), INRIA Sophia Antipolis (G. Barthe) and Université de Rennes (C. Bidan)

8.2. International Relationship

We have research activities with international partners as:

- Anthony Watson, Univ. Edith Cowan, Australie,
- Peter Honeyman, Univ. Michigan, USA,
- Piet Demeester, Univ. Gent, Belgium.

8.3. Visits and Invitations of Researchers

Ivan Stojmenovic from was invited in Lille for two month in June and July 2003.

9. Dissemination

9.1. Scientific Animation

David Simplot-Ryl is associate editor of *International Journal on Computers and Applications* (IASTED/Acta Press). He is guest-editor of several special issues: *IEEE Network Magazine* on "Ad Hoc Networking: Data Communications & Topology Control" to appear in July/August 2004, *Ad Hoc Networks* (Elsevier) on "Topology Control and Energy Efficient Network Protocols in Ad Hoc Networks" to appear in 2004, *International Journal on Wireless Mobile Computing* (Inderscience) on "Wireless Ad Hoc Networking" to appear in 2004. David Simplot-Ryl, Gilles Grimaud and Jean-Jacques Vandewalle are guest-editors of a special issue of *International Journal on Computers and Applications* (IASTED/Acta Press) on "System and Networking for Smart Objects" to appear in 2005.

David Simplot-Ryl is chairman of the *International Workshop on Wireless Ad Hoc Networking (WWAN 2004)*, (Tokyo, Japan, 2004) organized in conjunction with *24th IEEE International Conference on Distributed Computing Systems (ICDCS-2004)*.

David Simplot-Ryl is program committee member of several international events: *IEEE Third International Workshop on Wirelessq Local Networks (WLN 2003)*, (Bonn, Germany, 2003) organized in conjunction with *28th Annual IEEE Conference on Local Computer Networks (LCN 2003)*, *1st International Workshop on Objects Models and Multimedia Technologies (OMMT 2003)*, (Geneva, Switzerland, 2003) organized in conjunction with *9th International Conference on Object-Oriented Information Systems (OOIS-2003)*, *IFIP TC8 Working Conference on Mobile Information Systems (MOBIS)* (Oslo, Norway, 2004) and *First IEEE Internationation Conference on Mobile Ad-hoc and Sensor Systems (MASS 2004)* (Fort Lauderdale, USA, October 25-27, 2004). Gilles Grimaud and Jean-Jacques Vandewalle are PC members of *6th Smart Card Research & Advanced Application Conference (CARDIS'04)*, (Toulouse, France, 2004). Farid Nait-Abdesselam is PC member of *2004 International Conference in Internet Computing (IC'04)* (Las Vegas, Nevada, USA, June 21-24) and *2004 International Conference on Wireless Networks (ICWN'04)* (Las Vegas, Nevada, USA, June 21-24) to be held in conjunction with 2004 International MultiConference in Computer Science & Computer Engineering.

9.2. Teaching

David Simplot-Ryl is director of vocational master in computer science applied to enterprise management (IUP MIAGE) in continuous training. He is in charge of lecture in *Computer Organization and Architecture* for computer science degree (licence) and of lecture in *Mobile Networking* for research and professional masters in computer science (maîtrise, DEA, DESS).

Gilles Grimaud is in charge of lecture in *Embedded Systems* for research master (DEA), of lecture in *Security of Networks and Systems* for professional master (DESS), of lecture in *Operating Systems Architecture* for master of computer science (maîtrise), and of lecture in *Networking* in computer science degree (licence).

Jean Carle is in charge of lectures in *Networking and Data Communication* to under degree in computer science and vocational degree in computer science (IUT 2nd year/licence professionnelle).

Farid Nait-Abdesselam was responsible of the *Networks and Multimedia* option in the 5th year engineering degree in telecommunications at INSA of LYON. He is in charge of lectures in *Mobile and Multimedia Networking* for engineers in telecommunications at INSA of LYON, and of lectures in *Networking* for masters degree (DEA) at INSA of LYON.

9.3. Colloquium, seminars participations and invitations

Damien Deville and Gilles Grimaud are invited to talk at *Cassis International Workshop (Construction and Analysis of Safe, Secure and Interoperable Smart devices* (march 2003, Marseille, France).

10. Bibliography

Major publications by the team in recent years

[1] N. Agoulmine, F. Nait-Abdesselam, A. Serhrouchni. *QoS Management of Multimedia Services based on Active Agent Architecture.* in « Int. J. on Operable Communications Networks », number 2–4, volume 2, 2000, pages 199-212.

[2] D. Brienne, G. Grimaud, R. Kalinowski, M. Latteux, D. Simplot. *Procédé d'Identification d'Étiquettes Électroniques par Rondes Adaptatives.* International Patent WO0101326, 2000.

[3] J. Cartigny, F. Ingelrest, D. Simplot. *RNG Relay Subset Flooding Protocol in Mobile Ad-hoc Networks.* in « Int. J. on Foundations of Computer Science », number 2, volume 14, 2003, pages 253–265.

[4] J. Cartigny, F. Ingelrest, D. Simplot-Ryl, I. Stojmenovic. *Localized LMST and RNG Based Minimum-Energy Broadcast protocols in Ad-Hoc Networks.* in « Ad Hoc Networks », 2004, to appear.

[5] J. Cartigny, D. Simplot, I. Stojmenovic. *Localized Minimum-Energy Broadcasting in Ad-hoc Networks.* in « Proc. IEEE INFOCOM 2003 », San Francisco, USA, 2003.

[6] D. Deville, A. Galland, G. Grimaud, S. Jean. *Smart Card operating systems: Past, Present and Future.* in « Proc. 5th NORDU/USENIX Conf. », Västeras, Sweden, 2003.

[7] D. Deville, G. Grimaud. *Building an 'Impossible' verifier on a Java Card.* in « Proc. 2nd USENIX Workshop on Industrial Experiences with Systems Software (WIESS'02 », Boston, USA, 2002.

[8] G. Grimaud, J.-J. Vandewalle. *Introducing research issues for next generation Java-based smart card plateforms.* in « Proc. Smart Objects Conf. (sOc'2003) », Grenoble, France, 2003.

[9] F. Ingelrest, D. Simplot-Ryl, I. Stojmenovic. *Ressource Management in Wireless Networking.* Kluwer, 2004, chapter Energy Efficient Broadcasting in Wireless Mobile Ad Hoc Networks, to appear.

[10] F. Nait-Abdesselam, H. Koubaa. *Enhanced Routing-aware Adaptive MAC with Traffic Differentiation and Smoothed Contention Window in Wireless Ad-Hoc Networks.* in « Proc. 1st IEEE Workshop on Wireless Ad Hoc Networking (WWAN 2004) », Tokyo, Japan, 2004, to appear.

Doctoral dissertations and “Habilitation” theses

[11] J. Cartigny. *Contributions a la Diffusion dans les Reseaux Ad Hoc.* Ph. D. Thesis, Univ. Lille 1, December, 2003.

[12] D. Simplot. *Protocoles Reseaux pour la Gestion d’une Large Population de Petits Objets Portables et Securises.* Ph. D. Thesis, Univ. Lille 1, 2003, Habilitation Thesis.

Articles in referred journals and book chapters

[13] J. Carle, D. Simplot-Ryl. *Energy Efficient Area Monitoring by Sensor Networks.* in « IEEE Network Magazine », 2004, to appear.

[14] J. Cartigny, D. Simplot. *Border Norde Retransmission Based Probabilistic Broadcast Protocols in Ad-Hoc Networks.* in « Telecommunication Systems », number 1-4, volume 22, 2003, pages 189-204.

Publications in Conferences and Workshops

[15] A. Benlarbi-Delai, D. Simplot, J. Cartigny, J.-C. Cousin. *Using 3D indoor microwave phase sensitive stereoscopic location system to reduce energy consumption in wireless ad-hoc networks.* in « Proc. Smart Objects Conf. (sOc’2003) », Grenoble, France, 2003.

[16] J. Cartigny, D. Simplot. *Border Norde Retransmission Based Probabilistic Broadcast Protocols in Ad-Hoc Networks.* in « Proc. 36th Annual Hawaii Int. Conf. on System Sciences (HICSS-36) », Hawaii, USA, 2003.

[17] D. Deville, A. Courbot, G. Grimaud. *Extension temps-reel pour exo-noyau embarque.* in « Proc. 3e Conf. Francaise sur les Systemes d’Exploitation (CFSE) – French Chapter of ACM-SIGOPS », La Colle sur Loup, France, 2003.

[18] D. Deville, A. Galland, G. Grimaud, S. Jean. *Assesing the future of Smart Card operating systems.* in « Proc. Int. Conf. on Research in Smart Cards (E-Smart) », Sophia-Antipolis, France, 2003.

[19] D. Deville, G. Grimaud. *Compiling in the Very Small.* in « Proc. Int. Workshop on Construction and Analysis of Safe, Secure and Interoperable Smart devices (CASSIS’04) », 2004, to appear.

[20] M. Hauspie, D. Simplot, J. Carle. *Partition Detection in Ad-Hoc Networks Using Multiple Disjoint Paths Set.* in « Proc. of the 1st Int. Workshop on Objects Models and Multimedia Technologies (OMMT) », Geneva, Switzerland, 2003.

[21] M. Hauspie, D. Simplot, J. Carle. *Partition Detection in Mobile Ad-hoc Networks.* in « Proc. of the 2nd Mediterranean Workshop on Ad-Hoc Networks (MED-HOC-NET 2003) », Mahdia, Tunisia, 2003.

[22] H. KOUBAA, F. NAIT-ABDESSELAM. *Achieving Routing Based Medium Access Fairness in Wireless Ad-Hoc Networks.* in « Proc. 5th Int. Workshop on Distributed Computing (IWDC'03) », Kolkota, India, 2003.

[23] F. NAIT-ABDESSELAM, H. KOUBAA. *RAMAC: Routing-aware Adaptive MAC in IEEE 802.11 Wireless Ad-Hoc Networks.* in « Proc. 8th Int. Conf. on Cellular and Intelligent Communications (CIC'03) », Seoul, Korea, 2003.

Internal Reports

[24] J. CARTIGNY, D. SIMPLOT-RYL, I. STOJMENOVIC. *An adaptive localized scheme for energy-efficient broadcasting in ad hoc networks with directional antennas.* Technical report, number 2003-12, 2003.

Miscellaneous

[25] V. CORDONNIER, D. SIMPLOT. *Dispositif de Localisation d'un Objet Communicant dans une Population d'Objets Communicants et Objet Communicant Utilisé dans un tel Dispositif.* 2003, French patent 0306887.

[26] F. INGELREST, D. SIMPLOT-RYL, I. STOJMENOVIC. *Target Transmission Radius over LMST for Energy-Efficient Broadcast Protocol in Ad Hoc Networks.* 2003, submitted.

Bibliography in notes

[27] I. AKYILDIZ, W. SU, Y. SANKARASUBRAMANIAM, E. CAYIRCI. *Wireless Sensor Networks: a Survey.* in « Computer Networks », volume 38, 2002, pages 393–422.

[28] D. R. ENGLER, M. F. KAASHOEK. *Exterminate All Operating System Abstractions.* in « Proc. 5th IEEE Workshop on Hot Topics in Operating Systems », Orcas Island, USA, 1995.

[29] K. FINKENZELLER. *RFID Handbook: Radio-Frequency Identification Fundamentals and Applications.* John Willey & Sons, 1999.

[30] GEMPLUS/TAGSYS. *18000-3 Anti-collision protocol 13.56MHz RFID Tag.* ISO/IEC JTC 1/SC 1/GW 4/SG 3, 2002.

[31] M. ILYAS, editor, *The Handbook of Ad Hoc Wireless Networks.* CRC Press, 2003.

[32] *Java Card Web Site.* http://java.sun.com/products/javacard.

[33] N. LI, J. HOU, L. SHA. *Design and analysis of an MST-based topology control algorithm.* in « Proc. IEEE INFOCOM 2003 », San Francisco, USA, 2003.

[34] G. C. NECULA. *Proof-Carrying Code.* in « Proc. 24th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages », Paris, France, 1997.

[35] W. PENG, X. LU. *On the Reduction of Broadcast Redundancy in Mobile Ad Hoc Networks.* in « Proc. Annual Workshop on Mobile and Ad Hoc Networking and Computing (MOBIHOC 2000) », pages 129–130, Boston, Massachusetts, USA, August, 2000.

[36] C. PERKINS, editor, *Ad Hoc Networking.* Addison Wesley, 2001.

[37] A. QAYYUM, L. VIENNOT, A. LAOUITI. *Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks.* in « Proc. of the 35th Annual Hawaii Int. Conf. on System Sciences (HICSS-35) », Hawaii, 2002.

[38] I. STOJMENOVIĆ, editor, *Handbook of Wireless Networks and Mobile Computing.* John Wiley & Sons, 2002.

[39] I. STOJMENOVIC, M. SEDDIGH, J. ZUNIC. *Dominating sets and neighbor elimination based broadcasting algorithms in wireless networks.* in « IEEE Transactions on Parallel and Distributed Systems », number 1, volume 13, 2002, pages 14–25.

[40] C.-K. TOH. *Ad Hoc Mobile Wireless Networks: Protocols and Systems.* Prentice Hall, 2001.

[41] G. TOUSSAINT. *The relative neighborhood graph of finite planar set.* in « Pattern Recognition », number 4, volume 12, 1980, pages 261–268.

[42] J. WIESELTHIER, G. NGUYEN, A. EPHREMIDES. *On the construction of energy-efficient broadcast and multicast trees in wireless networks.* in « Proc. IEEE INFOCOM 2000 », pages 585–594, Tel Aviv, Israel, 2000.