Journal of Computer Networks and Communications

Privacy and Security in Wireless Sensor Networks: Protocols, Algorithms, and Efficient Architectures

Guest Editors: Sergio Saponara, Agusti Solanas, Gildas Avoine, and Bruno Neri

Privacy and Security in Wireless Sensor Networks: Protocols, Algorithms, and Efficient Architectures

Journal of Computer Networks and Communications

Privacy and Security in Wireless Sensor Networks: Protocols, Algorithms, and Efficient Architectures

Guest Editors: Sergio Saponara, Agusti Solanas, Gildas Avoine, and Bruno Neri

Editorial Board

Contents

Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2013, Article ID 528750, 3 pages
http://dx.doi.org/10.1155/2013/528750

Editorial

Privacy and Security in Wireless Sensor Networks: Protocols, Algorithms, and Efficient Architectures

Sergio Saponara,[1] Agusti Solanas,[2] Gildas Avoine,[3] and Bruno Neri[1]

[1] *Dipartimento di Ingegneria della Informazione, Università di Pisa, via G. Caruso 16, 56122 Pisa, Italy*
[2] *Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Av. Paisos Catalans 26, 43007 Tarragona, Spain*
[3] *Université Catholique de Louvain, Place Saint Barbe 2, Office Réaumur A.142, B-1348 Louvain-la-Neuve, Belgium*

Correspondence should be addressed to Sergio Saponara; sergio.saponara@iet.unipi.it

Received 18 February 2013; Accepted 18 February 2013

In the last years, Wireless Sensor Networks (WSNs) experienced a rapid growth with a huge interest from both academia and industry. Besides communication services, their applications include environmental monitoring, surveillance, logistics and process control in industrial scenarios, local and home area networks for health, assistance of elderly and disabled people, energy saving, smart homes, and/or smart city services.

The widespread deployment of WSN nodes and their interconnection through personal, local, or metropolitan area networks pose several challenges in terms of privacy and security of the network and of the access to data. Moreover, some of the possible applications of WSN have stringent security issues. Notwithstanding, this is only a part of the problem: the nodes of a WSN have limited resources in terms of computational and storage capability and have strict constraints in terms of compact size, low-power consumption, and power management. Therefore, new models, protocols, and advanced architectures for WSN have to be devised.

In the aforementioned context, the article by I. Coisel and T. Martin addresses the privacy concerns derived from the rise of wireless applications based on Radio Frequency Identification (RFID) technology. Indeed, nowadays when such an application is deployed, informed customers yearn for guarantees that their privacy will not be threatened. One formal way to perform this task is to assess the privacy level of the RFID application with a model. However, if the chosen model does not reflect the assumptions and requirements of the analyzed application, it may misevaluate its privacy level. Selecting the most appropriate model among all the existing ones is not an easy task. To this end, the article by I. Coisel and T. Martin investigates the eight most well-known RFID privacy models and thoroughly examines their advantages and drawbacks in three steps. Firstly, five RFID authentication protocols are analyzed with these models. This discloses a main worry: although these protocols intuitively ensure different privacy levels, no model is able to accurately distinguish them. Secondly, these models are grouped according to their features (e.g., tag corruption ability). This classification reveals the most appropriate candidate model(s) to be used for a privacy analysis when one of these features is especially required. Furthermore, it points out that none of the models is comprehensive. Hence, some combinations of features may not match any model. Finally, the privacy properties of the eight models are compared in order to provide an overview of their relations. This part highlights that no model globally outclasses the other ones. Considering the required properties of an application, the thorough study provided in this article aims at helping the system designer to choose the best suited model.

The article by C. S. Malavenda et al. reports the analysis, implementation, and experimental testing of a delay-tolerant and energy-aware protocol for a WSN node, oriented to security applications. The proposed solution takes advantages from different domains considering as a guideline the low-power consumption and facing the problems of seamless and lossy connectivity offered by the wireless medium along with very limited resources offered by a wireless network

node. After an overview of delay-tolerant wireless sensor networking (DTN), the article performs a simulation-based comparative analysis of state-of-the-art DTN approaches and illustrates the improvements offered by the proposed protocol. Finally, the experimental data gathered from the implementation of the proposed protocol on a proprietary hardware node are presented.

Network coding has attracted the attention of many researchers in security and cryptography. In the article by Y. Zhang and M. Minier, a selective forwarding attack is studied in network coding systems. While most of the literature has been dedicated to the countermeasures against pollution attacks where an attacker modifies intermediate packets, only few articles have focused on selective forwarding attacks on data or acknowledgment (ACK) packets; those last ones are required in network coding. However, selective forwarding attacks stay a real threat in resource constraint networks such as WSN, especially when selective forwarding attacks target the acknowledgment (ACK) messages, referred to as flooding attacks. In the latter model, an adversary can easily create congestion in the network and exhaust all the available resources. The degradation of the QoS (delay, energy) goes beyond the capabilities of cryptographic solutions. The paper by Y. Zhang and M. Minier first simulates and analyzes the effects of selective forwarding attacks on both data flows and ACK flows. Then it investigates the security capabilities of multipath acknowledgment.

The following articles are more focused on the application aspects of WSN and related to privacy/security issues; these articles address also architectural aspects and propose the implementation of some proof-of-concept hardware/software prototypes.

In modern houses, the presence of sensor and actuators is growing. Besides communication and entertainment systems, also advanced services are now arising; take as an example those for energy-saving and energy user awareness or those for medical assistance to the elderly or disabled people.

The utilization of wireless communication technologies, such as ZigBee, WiFi, and Bluetooth, is attractive because of their short installation times and low costs. Research is moving towards the integration of the various home appliances and devices into a single domotic system to be able to exploit the cooperation among the diverse subsystems and to provide the end user with a single multiservice platform. Obviously, privacy and security issues are arising together with the development of these new wireless home networks, particularly for the services related to the health assistance or the energy behavior of users. Such topics are addressed by the work of R. G. Garroppo et al., which presents the experimental evaluation of a domotic framework centered on a Session Initiation Protocol- (SIP-) based home gateway (SHG). While SIP is used to build a common control plane, the SHG is in charge of translating the user commands from and to the specific domotic languages. The analysis has been devoted to assess both the performance of the SHG software framework and the negative effects produced by the simultaneous interference among the three widespread wireless technologies: ZigBee, WiFi, and Bluetooth. A prototype of the SIP-based home gateway has been realized via software on a single-board computer with a Texas Instrument AM 3730 processor (ARM Cortex-A8 at 720 MHz), 256 MB of DRAM and 256 MB of flash memory plus a ZigBee module, a Hama Bluetooth adapter, and a WiFi card.

The architecture and the security issues of an energy home area network (HAN) for Smart Grid are addressed in the article by S. Saponara and T. Bacchillone. An implementation of the HAN is proposed, dealing with its security aspects and showing some solutions for realizing a wireless network based on ZigBee. Possible hardware-software architectures and implementations using Commercial Off-The-Shelf (COTS) components are presented for key building blocks of the energy HAN such as smart power meters and plugs, and a home smart information box providing energy management policy and supporting user's energy awareness.

The issue concerning domotic WSN for health applications is addressed in the work by M. Donati et al. The considerable impact on patient quality of life, the resources congestion, and the related costs due to monitoring of patients affected by chronic illness such as chronic heart failure (CHF) can be efficiently mitigated using remote wireless biosensor networks (WBSNs). The WBSN should be placed at patient home to be able to communicate in secure way over the public Internet with the cardiology departmental Hospital Information System (HIS). In this way, physicians can monitor the situation of several patients at distance and quickly detect alterations in vital parameters. In this scenario, the Health@Home (H@H) platform is conceived. The pool of Bluetooth sensors enables patients to daily collect vital signs at home in noninvasive fashion. A home gateway receives and processes all signals before sending them to a server node in charge of interfacing with the usual HIS. The novel concept of operating protocol (OP) represents a list of actions, remotely configurable, that the domestic network has to follow (required measurements, transmissions, comparisons with personalized thresholds, etc.). The first medical tests on 30 patients for 1 month allowed to verify the model, both from the patient and the medical perspectives. The main evaluation metrics were usability, flexibility, and reliability of the communication from sensors to HIS.

Finally, an industrial application of wireless technologies is addressed in the article by F. Iacopetti et al. The article presents wireless sensing systems to increase the safety and robustness in industrial process control, particularly in industrial machines for marble slab working. The experimented contactless sensing systems are based on RFID and capacitive technologies. Their application has the final aim of detecting the presence of a marble slab to be worked by the marble machine, at the machine entrance stage and in proximity of the working tools inside the machine. The proposed techniques aim at overcoming some limitations of the currently used slab detection systems, consisting in electromechanical or optical devices, suffering from deterioration and from the dirty and wet working environment. Slab detection at the entrance stage is needed for the determination of the slab shape, which is used by the machine controller to activate the abrasive or cutting heads only when the slab, transported on a conveyer belt, is present under each working

tool. Current industrial systems do not implement slab position detection inside the machine. Four RFID systems at 125 kHz, 13.56 MHz, 868 MHz, and 2.45 GHz and capacitive sensors exploiting two sensing approaches have been tested in several setups representative of the environment found in real marble machines. For the experimental test campaign with the RFID systems, commercially available tags, readers, and antennas have been used together with customized hardware and/or software. For the tests of capacitive sensing technologies, adhoc metallic plane capacitors or PCB-based ones plus the relevant frontend acquisition and conditioning circuitry have been realized. Compared to state-of-the-art sensing techniques, the proposed solutions allow for a reliable detection at the same time being of low complexity and robust to industrial environment harsh conditions. RFID tags and capacitive devices may be used for slab detection implementing a multipoint wireless or wired sensor network, whose output data need to be collected and transmitted to the main machine controller. For the safety of the overall working process, data integrity check and proper controller processing algorithms have to be implemented.

Sergio Saponara
Agusti Solanas
Gildas Avoine
Bruno Neri

Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2013, Article ID 781620, 12 pages
http://dx.doi.org/10.1155/2013/781620

Research Article

Operating Protocol and Networking Issues of a Telemedicine Platform Integrating from Wireless Home Sensors to the Hospital Information System

Massimiliano Donati,[1] Tony Bacchillone,[1] Luca Fanucci,[1] Sergio Saponara,[1] and Filippo Costalli[2]

[1] *Department of Information Engineering, University of Pisa and Consorzio Pisa Ricerche s.c.a.r.l, 16 G. Caruso Street, 56122 Pisa, Italy*
[2] *Caribel Programmazione S.r.l., 1 G. Malasoma Street, 56121 Pisa, Italy*

Correspondence should be addressed to Massimiliano Donati; m.donati@iet.unipi.it

Received 29 July 2012; Accepted 8 February 2013

Academic Editor: Bruno Neri

Chronic heart failure (CHF) is among the major causes of hospitalization for elderly citizens. Its considerable impact on patient quality of life, the resources congestion, and the related costs can be efficiently mitigated using remote wireless biosensors networks placed at patient home, able to communicate in secure way over the public Internet with the cardiology departmental Hospital Information System (HIS). In this way, physicians can monitor the situation of several patients at distance and quickly realize and act alterations in vital parameters. In this scenario, the Health@Home (H@H) platform is conceived. The pool of Bluetooth sensors enables patients to daily collect vital signs at home in noninvasive fashion. A home gateway receives and processes all signals before sending them to a server node in charge of interfacing with the usual HIS. The novel concept of operating protocol (OP) represents a list of actions, remotely configurable, that the domestic network has to follow (required measurements, transmissions, comparisons with personalized thresholds, etc.). The first medical tests on 30 patients (1 month) allowed to verify the model, both from the patient and the medical perspective. The main evaluation metrics were usability, flexibility, and reliability of the communication from sensors to HIS.

1. Introduction

Chronic heart failure represents one of the most relevant chronic diseases in all industrialized countries, affecting approximately 20 million people in Europe and US [1–3]. The hospital admissions, mainly concentrated in the older adults segment, range from a prevalence of 1.5% to 8.4% in 65–74 years and 75 years or older groups, respectively [2]. Admissions to hospital with heart failure have significantly doubled in the last 20 years [1]. Despite the advancements in medical and pharmacological fields, CHF continues to increase in both prevalence and incidence, with 4 million new cases each year in Europe and US, as result of the general ageing of population [4]. To address the societal and economical issues posed by the hospital admissions due to CHF [5] (2% of the total healthcare expenditure [6, 7], with hospitalizations that represent more than two-thirds of such expenditure [3]), the introduction of cost-efficient healthcare services/treatments is required, in particular preventive strategies aiming at more effective outpatient follow-up management programs [8].

It is acknowledged that the current healthcare model based on periodic visits, usually monthly, leads to a high re-hospitalization rate (25% within 30 days and 45% within 6 months [9]), failing to early detect the signs of destabilization. Besides the important problem of poor quality of life of surviving patients and their caregivers [10], this results in high congestion in specialized health facilities and poses financial problems to the National Health Systems. There is in the literature some evidence that a multidisciplinary management program [8, 11], including a home-based follow-up strategy, that is, telemonitoring or structured telephone support, can improve the outcomes of heart failure patients.

It provides a reduction in mortality, hospital readmissions, and lengths of hospital stays, and in general increases patient satisfaction [12–14].

The current ICTs (Information and Communication Technologies) enable to build effective telemonitoring systems, overcoming the limit of the actual models. Biomedical wireless sensors networks allow for a daily collection of interesting biological parameters at home. The increasing computational power available in numbers of embedded devices permits more and more complex signal processing algorithms, while large amounts of data can be safely moved globally via the Internet.

The Heatlh@Home (H@H) project introduces a new flexible and high configurable platform for domestic vital signs acquisition and processing, along with a management scheme able to support in an integrated and coordinated fashion the whole treatment of CHF patients since their enrolment in the system. Being directly integrated with the usual cardiology departmental HIS, the H@H platform aims at connecting in-hospital care of the acute syndrome with out-of-hospital followup by patient/family caregiver. Patients' signs, symptoms, and raised alarms can be received remotely by the healthcare providers, and aggravations can be quickly detected and addressed. More frequent (usually daily) assessment of clinical parameters than in conventional practice is permitted [15]. The benefits extend beyond the early detection of clinical destabilization: better and optimized scheduling of specialized resources and reduction of unnecessary travel to hospital.

Hereafter, Section 2 reviews the state of the art. The H@H system architecture is introduced in Section 3. Sections 4, 5, and 6 describe respectively the sensing devices, the home gateway and the collection server. Communication details are explained in Section 7. Section 8 describes the testing validation phase. Conclusions are drawn in Section 9.

2. State of the Art Review for Telemedicine Systems

Considering the Ambient Assisted Living (AAL) roadmap [16] that draws the guidelines to develop efficient strategies and systems to face the aging of population, along with future challenges in telecare [17] and some recent studies on AAL solutions [18], especially for telemonitoring [19], the desirable features of a monitoring platform for chronic disease are as follows:

(1) health monitoring service using wearable/portable sensors for non-invasive measure of vital signs, activity level and symptoms signaling,

(2) reasoning and data processing to detect emergency situations or behaviors,

(3) secure and reliable communication of data,

(4) interconnection between stationary home care and acute medical treatment,

(5) integration with existing solutions and components,

(6) modular structure of the solution to ensure easy maintenance and future extensions,

(7) high degree of interoperability accomplished by the use of well-known communication standards,

(8) flexibility to face the wide range of patients' status and the progress of chronic diseases,

(9) interfaces and system requirements defined taking into account the individuality of the end user group.

Today there are many system of telemedicine [20–27] specific for CHF or suitable for this kind of disease, together with many dedicated prototypes and project trial [28–30]. However, at the state-of-the-art, it is difficult to find a solution that completely agrees with all the previous requirements. Systems based on telephone calls or web-portal to report symptoms and outcomes of the measures have to be discarded for scalability and usability issues. Considering instead systems in which measures are performed by the patient and automatically transmitted to remote node, most of them use a dedicated collection database failing the requirement point 4 and partially the point 5. This way data collected at home are not flowed into the existing HIS that in turn contains only data related to acute syndrome. All solutions have a gateway that at least receives and forwards data coming from sensors. Sometimes signal processing and reminders are provided. This device is often realized using a smartphone or tablet, a set-of-box or a PC. However their mall screens and rich application interfaces do not meet the requirements of older users (>65 years and often with comorbidity and cognitive or sensorial deficit), lowering the acceptance/usability of the system. Finally, all considered systems do not include a formal method to adapt and monitor the follow-up activities to be performed at home by the patient. The H@H telecare platform, described in detail in the following sections, represents a complete and high configurable ICT solution for CHF remote management, developed taking into consideration all the guidelines discussed in the above points to overcome the limits of the state of the art.

3. H@H Telecare System and Networking Overview

The requirements of the system come from a close collaboration among important healthcare providers (Hospitales Virgen del Rocio, Spain; Dom Koper Hospital in Slovenia and the research clinical center Fondazione Gabriele Monasterio in Italy) and technical entities within the H@H consortium. This multidisciplinary approach leads to develop a platform able to meet medical expectation, patient's features (elderly, with numerous comorbidity and cognitive deficit), and the progressive nature of the disease.

The key points of the proposed architecture are two. Firstly the concept of follow-up operating protocol (OP) as embed formal description of the medical prescription and definition of the behavior of the home system. Secondary, the native integration with the HIS which is already present in most cardiology departments. Other interesting features are the reduced impact on the patient due to the limited effort required to follow the assigned therapy and the low overhead introduced with respect to the regular activity of medical staff.

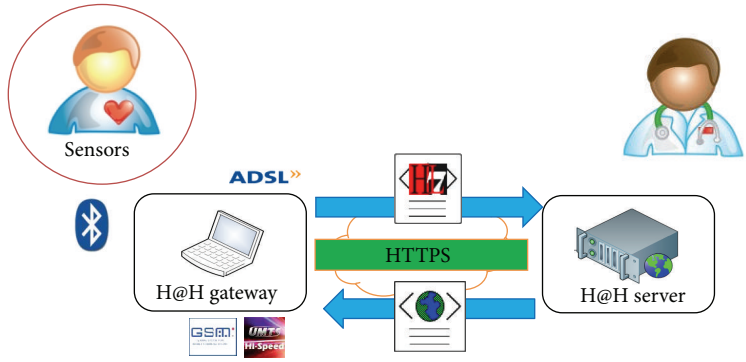


Figure 1: H@H system architecture.

	WiFi	IrDA	Bluetooth	ZigBee
Data rate	Excessive	Ok	Ok	Ok
Power consumption	Ko	Ok	Ok	Ok
Presence on the market	Ok	Ok	Ok	Ko
Distance	Ok	Ko	Ok	Ok
Line-of-sight required	No	Yes	No	No

Figure 2: Comparison among wireless technologies for sensor network communication.

From the architectural point of view, the global system follows the client/server paradigm (see Figure 1). At patient's home, a set of wireless biosensors allows to measure the main vital signs while the home gateway centralizes all computation and communication resources, masking the complexity of the sensors network to the server. The latter, installed at health service facilities, accepts and processes data from several gateways making them available in the HIS and finally allows the management of all patients since their enrolment. This hierarchical structure improves the scalability and the upgrading of the system.

Biomedical sensors that form the network are equipped with wireless connectivity in order to submit acquired data to the home gateway. In that sense Bluetooth 2.0 technology represents the better tradeoff among available bandwidth (430 Kbps against ~18 Kbps required by the ECG-SpO2 device), security and reliability of the connection (SAFER encryption algorithm), cost and power consumption of the node, link distance. Comparison among Bluetooth and the rest of possible communication technologies is shown in Figure 2.

The home gateway behaves as a server in the wireless sensors network located at the patient's home. It receives data from sensors over point-to-point connections, managing in time-division way the communication resource. Specific signal processing algorithms executed on incoming values allow to timely detect alterations in punctual values and trends over short and medium periods. The final step consists of forwarding elaborated data to the hospital server to be further analyzed and stored into the Electronic Health Record (EHR).

To accomplish the transmission task, multiple available technologies ensure a good adaptability of the system in overall operating areas. As outcome of the survey illustrated in Figure 3, the home gateway exploits both ADSL (via Ethernet or WiFi) and mobile broadband connectivity. The GSM global coverage of 99% gives a very high degree of connectivity, dealing also with digital divide issues because in the worst case the GPRS upload data rate of 20 Kbps is sufficient to transmit data in few minutes. Furthermore, the gateway leverages the GSM capability to send SMSs to the physician, patient's relatives, and caregivers in case of alarm situations.

Because of the personal nature of the data in transit, the privacy is a primary goal to achieve, avoiding that eavesdroppers could understand the content of the communications. Different protocols ensure simultaneously authentication, integrity, and confidentiality: IPSec, SSL/TSL, HTTPS, symmetric protocols. The chosen HTTPS relies on SSL connection and allows to exchange HTTP messages over a secure channels. It comes natively with all operating systems and does not require any further configuration other than the SSL certificate installation.

Finally, H@H involves international and well-known formats for data representation to definitively improve the interoperability of the system and the integration with existing HIS. The ANSI HL7-RIM Clinical Document Architecture (CDA) v2 [31–33] and XML codify, respectively, the post-processed vital signals and the current OP.

4. Wireless Sensors

The sensing elements of the domestic network are wireless biomedical devices selected with the rationale to minimize the impact on the patient, in order to be easily used autonomously by the patient at home. According to the analysis carried out by the physicians, the sensors in the H@H system are wearable/portable, noninvasivity, wireless [34], and battery powered. Additionally, to meet the peculiar patient features, the measurement experience consists of wearing/using the sensors only for the duration of the acquisition,

	ADSL	GSM	UMTS HSPA	wimax
Coverage	• Urban: Ok • Sub-urban: Ok • Rural: ~Ok	• Urban: Ok • Sub-urban: Ok • Rural: ~Ok	• Urban: Ok • Sub-urban: ~Ko • Rural: Ko	Ko
Data rate	Ok	Ok	Ok	Ok
Contract	• Fixed fee • Pay-per-use	• SMS: Pay-per-use • Data: Pay-per-use and fixed fee	• SMS: Pay-per-use • Data: Pay-per-use and fixed fee	• Fixed fee • Pay-per-use

Figure 3: Comparison among communication technologies for home gateway.

without any long-term installation of electrodes or other reading terminals. Low quality signals arising from sensors mispositioning are detected and requested again. Indeed signal quality is not excessively dependent on transducer positioning (e.g., 3-lead ECG instead of a more complex 12-lead ECG is adopted, as in [35]).

The significant vital parameters to monitor in a CHF patient (ECG, SpO2, weight, blood pressure, chest impedance, respiration, and posture) have been clustered into two possible configurations: basic and advanced. Basic partitioning implements the minimum set of requirements to achieve a complete telecare system, while the advanced version integrates additional features to widen the kind of CHF patients to be enrolled into the service and to cope with other chronic diseases (i.e., chronic obstructive pulmonary disease, diabetes). Table 1 shows the features of the sensors and the composition of the basic and advanced version of the system.

The basic version of the H@H monitoring system, used for the demonstration phase, envisages the use of three sensing devices (see Figure 4).

(i) The commercial UA-767BT arm cuff device for blood pressure readings by A&D Medical. The sensibility range and the accuracy are 20–280 mmHg and ±3 mmHg respectively. It outputs packets with 8 bit values of systolic and diastolic pressure and heart rate.

(ii) The commercial UA-321PBT digital scale by the same manufacturer for body mass measurements. It has a maximum capacity of 200 Kg and an accuracy of ±0.1 Kg. The value of the current body mass can be calculated from the 5 bytes data packets.

(iii) The ECG-SpO2 sensing module for acquiring synchronized 3-lead ECG, SpO2 and plethysmographic traces, developed ad hoc in the H@H project and detailed by the authors in [36]. Conditioned and digitalized (at 500 samples/s) ECG waveforms of two standard limb leads, level of oxygen saturation in the blood, digitalized (at 100 samples/s) plethysmographic waveform are sent in real time during the acquisition.

The latter device is assembled on a single 90 × 14 mm printed circuit board, hosting the CARDIC integrated circuit

Table 1: Home gateway sensor resources.

Parameters	Sampling	Basic	Advanced
3 lead ECG	500 S/s/lead (12 bit/S)	√	√
SpO2	3 S/s (10 bit/S)	√	√
Blood pressure	1 S/type (32 bit int)	√	√
Weight	1 S (32 bit float)	√	√
Chest imp	25 S/s (10 bit/S)		√
Respiration	25 S/s (10 bit/S)		√
Posture	3 axes × 1 S/s/axis (8 bit/S)		√

[36] to read 12 bit resolution ECG leads, the ChipOx OEM by Envitec which provides SpO2 readings and a digitalized plethysmographic waveform (measurement range from 45% to 100%, with an accuracy of 1.5–2% for oxygen saturation and measurement range 0–255 LSB with an accuracy of 6 ppm/LSB for plethysmography), the Bluetooth 2.0 chip OEMSPA312i by Connect Blue and the MSP430F2418 Ultra-Low Power Mixed Signal Controller for mixing raw data before passing them to the Bluetooth interface. Integrating ECG and SpO2 functionalities in a novel single sensor reduces the number of devices in the final system and also enables for advanced analysis (e.g., the Pulse Transit Time estimation) using synchronization between SpO2 and ECG traces. The sensor naturally allows to deal with a single parameter at a time.

All sensing devices send only raw data exploiting the onboard Bluetooth 2.0 Class I transceiver and data signal processing is completely demanded to the home gateway. They use the Service Discovery Protocol (SDP) and the Serial Port Profile (SPP) services to wirelessly communicate with the gateway, which acts as access point. PIN-based peering procedure is required once at configuration time, while during the permanence at patient's home the wireless sensors network not require further configurations (device searches, PIN validations, etc). Indeed each sensor acts as initiator of connections towards the home gateway when activated. This means that a measure acquisition simply consists of turning on the sensing device and waiting until the end of the measurement process without any preventive interactions, introducing also benefits in battery saving. Only one active connection at a time can be managed by the implemented home gateway, while simultaneous connection attempts lead

Figure 4: Wireless sensors for the basic version of the H@H system.

to discard attempts other than the first. This is not a real limitation since measurements have to be done one by one by the user.

5. Home Gateway and Operating Protocol

5.1. Home Gateway HW/SW Platform. The home gateway is the elaboration and communication node of the wireless sensors network. Centralizing and automating the acquisition and transmission of vital signs, it minimizes patient efforts. The gateway accepts incoming connections over the Bluetooth channel and handles all sensor-dependent communication protocols to receive data packets from the biomedical sensors and to extract their content. Its primary task is the data processing for early detection of critical alterations and the secure forwarding of the computation results (i.e., filtered data, alarms, etc.) to the remote server system to be further analyzed and finally flowed into the cardiology departmental HIS. The system provides a permanent storage of pending data waiting for transmission so that power supply failures do not result in data loss (16 MB, for 1 week complete acquisitions). With respect to the remote server the gateway masks the complexity and the heterogeneity of the sensors network behind it.

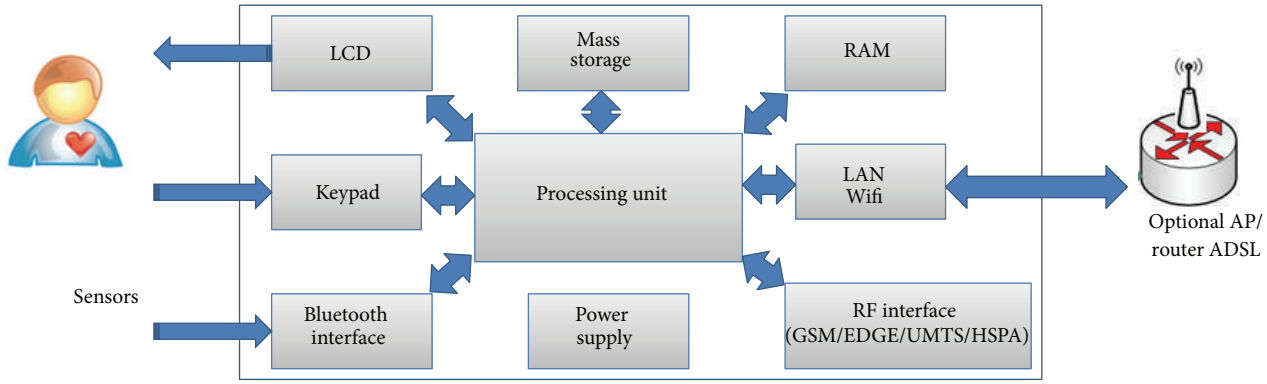
The gateway follows the OP and guides step by step the patient in performing the activities as scheduled by the physician, leveraging its powerful graphical user interface. In addition to the planned measures the system can receive others spontaneously performed by the patient. In this case it asks to select the reason of the measurement from a list, still ensuring the analysis process. Finally it is possible to submit alarms manually from a selectable list (i.e., dyspnoea, palpitation, breathlessness, etc.).

To achieve a fully compliance of requirements, taking into account flexibility, robustness, and user-friendliness, and at the same time reducing costs and project risks, several hardware solutions have been considered. Full custom platform presents some advantages but long development/testing time. Moreover, the number of devices for early demonstration is very low, resulting in a high cost per unit. Mobile phone has too small display and keys, limited memory space and comes with only mobile broadband connectivity. In smartphone potentially the allocation of memory and the computational resources meet the demands. However, it is not the better solution due to the size of display and also because, being born to telephony, running applications are placed on hold/delayed status in case of incoming call. Bluetooth access points are typically used to realize Bluetooth network in proximity marketing. Some of them allow customizing its functionality thanks to a Linux software platform and specific SDKs. These products are upgradeable with a series of interfaces with USB connection such as GSM/UMTS or Wifi modules. The degree of customization reachable without incurring the cost of SDK, inferred by tests, is not adequate for the project needs.

A netbook represents the best tradeoff among all metrics. Designed for wireless services it typically includes most of the needed resources: Bluetooth, Wifi, modem, 9-10 inches screen, speakers, low-power ×86—compatible processor, storage space. All missing interfaces, or future extensions, can be added by USB connector. The only drawback is the keyboard, whose keys are too small and too many with respect to the request. So in replacement of the native keyboard, a custom one was developed for the selected netbook (Samsung N150), including only the required buttons: Yes, No, Alarm sending, and Up/Down scroll buttons (see Figure 5).

Intel ATOM N450 1,66 GHz
Memory RAM 1 GB DDR2
Hard Disk Sata 250 GB
Display 10, 1″
Ethernet 10/100 LAN
Wireless 802.11 bg/n
Bluetooth 2.0
GSM/GPRS/EDGE and UMTS/HSPA
Bulit-in audio
Ad hoc 5 keys keypad

(a)



(b)

Figure 5: Home gateway architecture and hardware resources.

The operating system chosen for the gateway is based on Linux kernel 2.6.27 or higher, customized with the addition of a lightweight window manager and deprived of unnecessary services, applications, and kernel modules. The H@H software runs directly when netbook is switched on. It is implemented in C language using, respectively, libbluetooth, libSSL, libXML, libgtk to support Bluetooth management, security, XML parsing, and graphical development.

The software architecture is represented in Figure 6 using an UML diagram:

(i) the sensor server manages incoming connections over Bluetooth interface to receive raw data from sensors,

(ii) the network communicator manages the available channels to forward both collected information to the server and alert SMS to caregivers/physicians,

(iii) the clock and the scheduler ensure scheduling and reminder of all the therapeutic activities,

(iv) the graphical user interface handles both events throw during interaction with the keypad and the visualization of messages in the application window.

The main concerns of the system were implemented in separated threads to ensure a high modularity and the maximum flexibility when combining them in any arbitrary operating protocol. This modular architecture ensures easy maintenance and upgrades, including future extensions with new sensors or the introduction of new communication standards.

5.2. Operating Protocol. The newly developed OP concept consists of a set of actions, like taking measurements or replying to simple questions, that the patient must follow during the monitoring period as well as it completely defines the behavior of the home gateway in terms of types and frequencies of measurements transmission policy, selectable symptoms, comparison thresholds, and phone numbers for each alarm. The OP is tailored by the physician at the beginning of the monitoring period and it can be remotely updated in progress according to the patient conditions. In fact at the end of any data transmission, if necessary, the server is able to update the current operating protocol by sending the new one to the interested gateway. The OP update and the consequently reconfiguration of the gateway is totally transparent to the user. Usual values for measuring

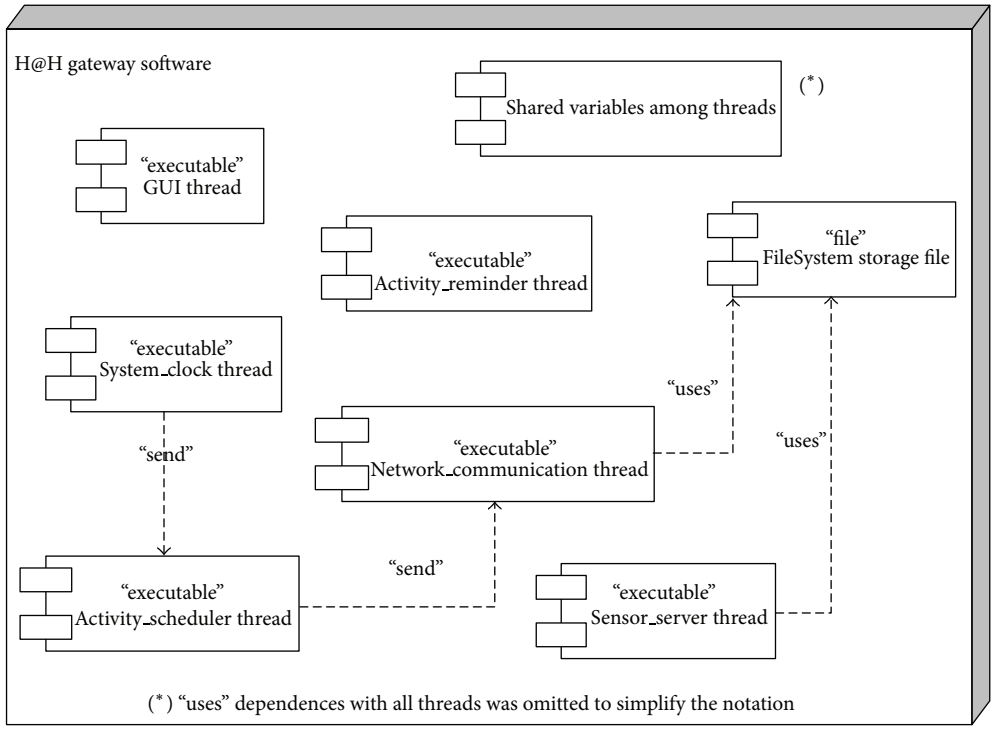


Figure 6: Components diagram of the gateway application software.

Table 2: The operating protocol.

Data	Schedule	Alarm level
3 lead ECG	1-2/day (5 min)	50 < HR < 100 bpm
SpO2	1-2/day (5 min)	>90%
Blood pressure	2-3/day	85 < sys < 160 mmHg 50 < dia < 100 mmHg
Weight	1-2/day	Gain < 1 kg/day Gain < 3 kg/week
Chest imp	1/day (5 min)	Fluctuation < 30%
Respiration	1/day (5 min)	12 < R < 25 bpm
Posture	Continuous	No activity/fall
Therapy reminder	1-2/day	3 faults in a week

frequencies and ranges for alarms detection are shown in Table 2, but clinicians can configure each parameter.

5.3. Data Processing and Alarm Management. Sensor data signal processing, implemented in the home gateway, is in charge of detecting alterations in vital signs potentially dangerous for the patient. In this way the physicians are timely alerted if anything out of the ordinary is found and they have in the HIS all patients' data to plan the following actions. Data processing involves three main steps: preprocessing, analysis and cry wolf avoidance. The preprocessing consists of the filtering of raw data provided by the sensors, removal of noise and main interference, and the extraction of derived information. The analysis step compares the outcome of the preprocessing with the thresholds defined in the OP that establish the admissibility range for punctual values or trends over a medium period. The last step is useful to reduce the number of false positive alarms, for example due to temporary stress or sensors misuse. In the presence of abnormal values, the same measurement is shortly deferred and only if the condition is confirmed the gateway raises the alarm, contacting caregiver or health professionals via SMS. The required arithmetic precision is compliant with real-time implementation on 32-bit single-core processor and the RAM memory available in the netbook. All involved algorithms have a linear complexity with the number of considered samples of the signal, both in terms of memory and computational cycles.

The electrocardiographic signal is treated to extract maximum, minimum, and average heart rate over the track as well as to detect the presence of atrial fibrillation. The reference point within the ECG signal is the QRS complex: three deflections that occur periodically and in rapid succession, where the R point represents the main upward ones. A derivative-based algorithm [37] and a rule-based system [38] for the QRS complex detection are applied. The source signal is filtered in order to keep just the central frequencies (8 to 30 Hz) where the QRS complex information lays. Afterwards, the signal is differentiated, squared, and averaged. Comparing the averaged signal against a threshold creates a set of windows that allow to recognize the R peaks in the filtered signal (maximum positive within the window). The R peak has still passed through a rule-based system that evaluates whether the detected QRS is a valid QRS complex or not

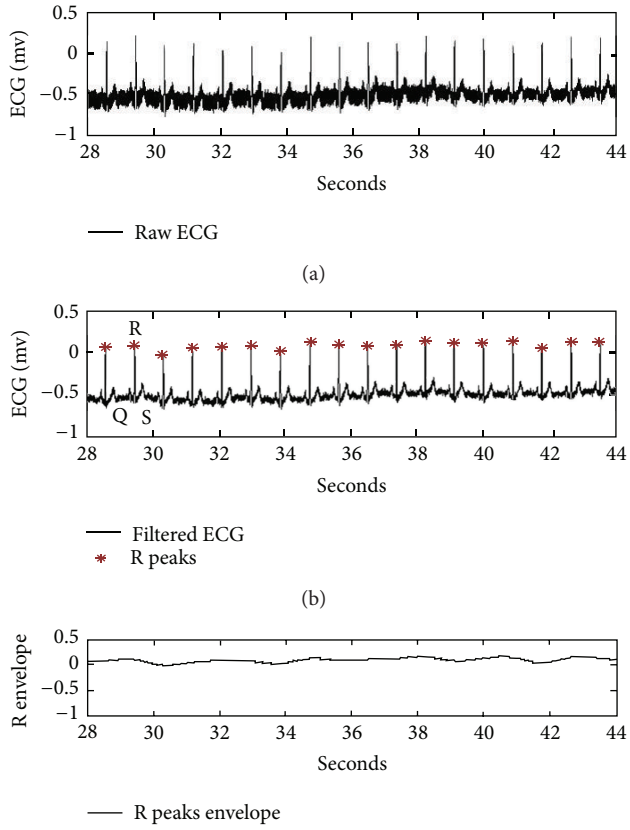


Figure 7: (a) Raw ECG signal corrupted by powerline noise; (b) filtered ECG signal and valid R peaks detected by the processing algorithm; (c) envelope signal of the valid R peaks.

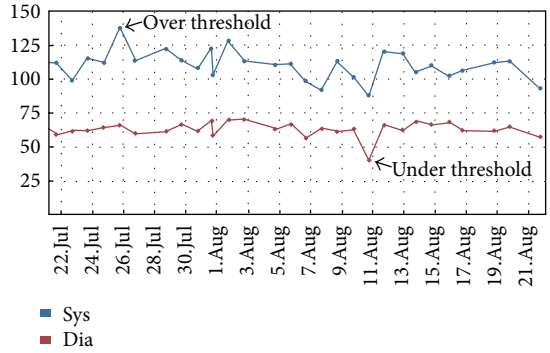


Figure 8: Example of blood pressure analysis of H@H.

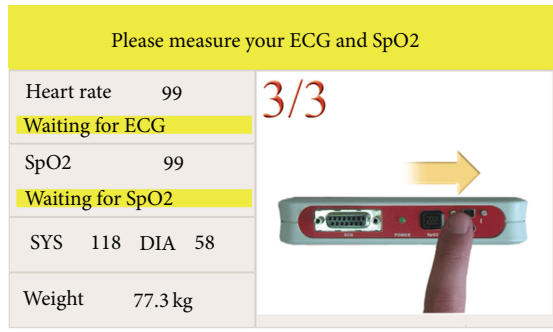


Figure 9: Example of the graphical user interface requesting a measurement.

based on the distance in time between consecutive peaks. To improve the legibility of the track for further medical review, a 50 Hz notch filter is applied to the signal to remove power-line noise. Figures 7(a) and 7(b) show the raw and filtered signal. There is also a cubic spline data interpolation algorithm that extracts the envelope of the R peaks as an indirect indication of the respiratory activity. Figure 7(c) shows the envelope signal of the peaks. The analysis of the intervals between consecutive R peaks, using a 30 seconds window shifted along the time axis by 5 seconds length steps [39], allows to calculate the heart rate.

Concerning SpO2 signal analysis, relevant values are maximum, minimum, and also the average level of oxygen saturation over the track, extracted by a digital low-pass FIR filter. The normal range in healthy people is from 94% to 100% while oxygenation can quickly lower in CHF patients; hence, a frequent monitoring is necessary to detect these changes.

Concerning blood pressure signal processing, systolic and diastolic values are analyzed (see Figure 8) to find out under or over threshold situations and the general trends of both parameters are verified looking for suspicious variability that are typical manifestation of cardiac instability.

As far as weight, this parameter is easy to measure and elaborate as well as very effective in the CHF management. It allows to detect fluid retention in the patient. The system is able to find out increases of 1 Kg in a day or 3 Kg in a week that are considered potentially critical situations in CHF.

5.4. User Interface. The user interface has an essential role in this application having to guide the patient in following the scheduled measurements or drugs assumptions. The developed home gateway provides an intuitive user interface able to display guide images, reminder messages, and sounds when a planned activity time is reached. Figure 9 shows the appearance of the graphical interface. Patients can read the last measured values of weight, blood pressure, heart rate, and oxygen saturation. At the top of Figure 9 the reminder textbox indicates the requested activity, along with the graphical helper that shows the correct actions to be done as gif animation. The other textboxes report the status of the related sensor, included battery charge. Green, yellow, and red textboxes background colors are used for information, warning, and error messages, respectively. In idle state the time of the next activity is visualized. The custom keypad allows to navigate and confirm symptoms in case of manual alarm or extra measure and to answer questions about pills therapy.

The gateway provides also the possibility to store in a local database all collected vital signs occupying less than 1 GB for one year observation. This functionality allows to select and visualize ECG tracks, R-Wave envelops, SpO2 tracks, and

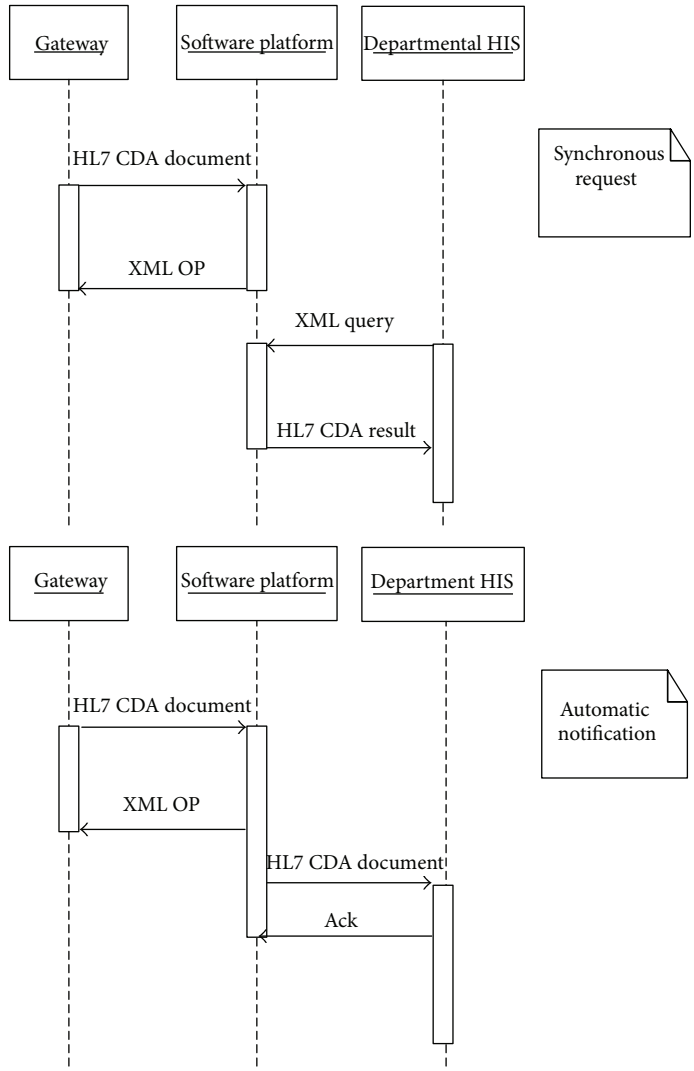


Figure 10: Methods of integration between the H@H software platform (server side) and the departmental HIS. The communication between the H@H home gateway and the server software platform is the same in both cases.

plethysmographic waves or trend graphs for weight, blood pressure, heart rate and SpO2. This is particular useful when medical staff is present at patient's home and needs to consult the measurements repository on-site.

6. Remote Server Module

The H@H server platform is a web-based application that receives data from gateways, providing a detailed process of analysis based on expert systems and finally the update of the patient record in the departmental HIS. No summarization function is provided, but it deals with all the received unaggregated data. Moreover the H@H server platform exports interfaces that allow the clinicians to interact with the system, retrieve information and manage all patients.

The format of data shared between the H@H server and the HIS is the ANSI HL7-RIM CDA v2, the same template adopted for the communications gateway-server. Besides HL7 CDA v2 is also possible to use other XML formats. Transmissions leverage the web services architecture and MLLP (Minimum Low Level Protocol) is applicable.

Two possible ways of integration with existing HIS are available (see Figure 10) in order to improve the interoperability of the system. In the first mode, called synchronous request (SR), all data are stored locally in the H@H server platform and vital signs are provided on-demand as result of query messages submitted from the HIS. Queries address a dedicated service endpoint and use XML to specify the searching parameters: the patient identification, the vital signs, and the time interval. In the SR mode a specific interface to build the queries has to be added to the HIS. The second mode, the automatic notification (AN) method, requires that the HIS interested in receiving the clinical information coming from the gateways exposes a dedicated webservice reachable by the H@H software platform. When new data are received and stored in the H@H server, they are immediately flowed to the registered HIS, enabling an automatic update of the EHR.

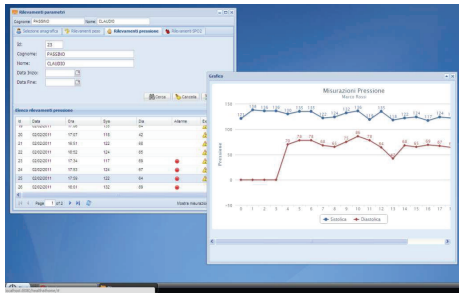


Figure 11: Appearance of the physician frontend.

From the functional point of view the software platform is composed of two main parts: the core and the frontend.

The frontend represents the human machine interface for the physicians (see Figure 11). Its main functions are related to the patient management since their enrolment, when the physician inserts the patient data and configures his OP. To be noted that user interfaces at both home gateway and server sides have been realized in different languages (English, Italian, Slovenian, Spanish) to allow the installation of the system in the National Health Systems of the different project partners. At any time the physician is able to look through the patient clinical folder, comparing the patient health status in different periods by means of measurement trends. The system is able to highlight the alarms encountered during the monitoring. If necessary the physician can modify the OP at any time, this produces an automatic and transparent update of the gateway. The frontend is based on the rich client technology which allows defining a simple user interface with high performance from the user interactivity point of view. The architecture is able to completely decouple application logic from data displaying, in order to make the interface fast, flexible, and usable by the user. Conceptually, the browser provides the features of a desktop application accessible from the Internet without installing any add-on. The visual components, written in Java Script, are downloaded at runtime and run locally into the browser.

The core part is based on the Spring Framework [40] which accepts patient measurements collected and sent by the gateways through a dedicated webservice endpoint. All received messages are formally verified and the contained observations are stored in the local database. The core is also in charge of managing the integration with the HIS, both serving the incoming queries in SR mode or forwarding vital signs to HIS in AN mode. Additionally the core is responsible for data retrieval when requested by the frontend. Data between the core and the frontend is exchanged through Java Script Object Notation. Finally the core exposes an additional service useful when a gateway has to be customized for new users.

7. Gateway-Server Networking

WAN (Wide Area Network) technologies, ADSL, or mobile broadband are used to communicate with the collection server. As data exchanged between gateway and server involves the public Internet, the use of HTTPS protocol fits completely the requirements of confidentiality, authenticity, and integrity for the data traffic. The protocol also meets perfectly the web service paradigm: the request message contains all pending results and events within its body, coded according to the HL7-RIM CDA v2, while the response includes the XML description of the current OP, allowing remote updates after each transmission.

The header of the CDA document contains information about the patient, used to address its EHR, and the recipient hospital. Result and Vital Signs sections contain numeric and waveform observation blocks, one for each measure. The *InterpretationCode* tag is used to mark normal or abnormal values. Symptoms are hosted as event observations in the Purpose section. Medical equipment section describes the sensing devices used. All observations use SNOME CT [41] or LOINC [42] codes.

Transmission occurs according to the OP, at the end of an activity, or on time-base (i.e., daily or weekly), and always after an alarm either manually signaled or automatically detected.

Communication occurs also when the gateway has to be configured for a new patient. A dedicated interface allows to completely configure the home gateway or to modify the current patient's information status, server IP addresses and ports, names of the collection and configuration service, and regionalization. The gateway contacts the configuration endpoint indicating the patient's ID. The server replies with all the information of the given patient and the personal OP. Now the configuration is complete, the reachability of the endpoints is tested and the monitoring can start. Using this procedure, patient information and operating protocol are defined only once at server-side, reducing the possibility of mistakes.

8. H@H Telecare System Testing

One of the key issues for the adoption of new telemedicine systems is an exhaustive mixed HW/SW test [43, 44]. The H@H system follows a very structured and incremental testing procedure concluded with the final technical validation and demonstration phase. Unit test of hardware components and operational correctness of software and firmware applications using conventional procedures were the first steps. The following integration test verified the end-to-end communication in the system and the overall system-level interactions of the different HW and SW parts. To this aim some ad hoc prepared scenarios and the involvement of healthy users were used. The last important phase before the final technical demonstration was the alpha-testing: two patients minimally aware of ICT and younger than the CHF average age (1 month). The first impressions of physicians and patients coming from these tests made possible to tune the final version of the system.

The technical validation of the H@H platform involved 30 patients with CHF disease in New York Heart Association (NYHA) classes III and IV, with an average age of 62 years,

hospitalized for acute heart failure in the previous 6 months and consenting to take part in the study. Acute coronary syndrome within 3 months before the enrolment was the only exclusion criteria. The size of the set of CHF affected patients is similar to those of other works published in the literature about ICT systems for CHF monitoring [45]. The minimum period of monitoring was one month.

The metrics established for the evaluation of the system belong to two main categories: objective and subjective. The first ones are related to items unequivocally measurable, the latter depend on the personal experience during the demonstration and the feeling with the system. A specific testing protocol and a questionnaire to collect patients, caregivers, and physicians feedbacks were used to validate the system. A group of selected cardiologist checked out the information arrival in HIS, evaluating the quality and coherence of data collected and the relevance of the alarms. The ergonomic of patient's interface was evaluated as a key point of system functionalities, as well as the general end-user usability. On the other hand the robustness and reliability of data transmission and the effectiveness from the medical point of view were evaluated.

The results show a very limited number of activity misses (<3%), mostly in the first days of monitoring. Moreover, the number of false positive alarms is less than 5%. No connectivity and transmission problems occurred, including data or sensors network configuration lost. Thanks to the high quality of acquired signals and alarms detection capability the physicians reported a valid impression of the system to control at distance the evolution of the followed patients. All physicians involved in the demonstration are definitively in favor of the adoption of the H@H system. 89% of the patients report a very high satisfaction level, motivating their choice with the friendliness of the solution and the easiness to follow the therapy.

The complete success of the H@H technology test under medical control led to plan a clinical validation (with OPEX/CAPEX economical analysis), including 500 patients in the Italian Regional Tuscany Health System.

9. Conclusions

The technologies currently available allow for the provisioning of effective out-of-hospital telemonitoring strategies for chronic diseases, instead of the actual in-hospital-based follow-up procedure based on periodic visits. In this scenario the H@H system proposes an innovative home care model for the CHF patients based on a Bluetooth wireless sensors network equipped with software tools and communication technologies for remote acquisition, analysis, and secure transmission of the main vital signs. The final aim is to design an integrated platform to support the whole process of the patient treatment, connecting in-hospital care with out-of-hospital followup. The system was developed around an OP with a per-patient granularity allowing to generate a really meaningful database for every patient. The use of international standards for data exchange and the well-know communication protocols improves the interoperability, favoring the future integration of the platform with other HIS or sensors.

All metrics about usability, reliability, and robustness of the platform evaluated during the first technology assessment in a real medical scenario, with tens of patients affected by CHF disease NYHA classes III and IV, prove the effectiveness of the H@H telemonitoring system from both the patients and the caregivers' point of view.

Acknowledgment

This work was supported by the Ambient Assisted Living Programme.

References

[1] "SHAPE survey results to the general public," in *Proceedings of the Annual Congress of the European Society of Cardiology*, Vienna, Austria, September 2003.

[2] F. Zannad, N. Agrinier, and F. Alla, "Heart failure burden and therapy," *Europace*, vol. 11, no. 5, pp. 1–9, 2009.

[3] V. L. Roger, A. S. Go, D. M. Lloyd-Jones et al., "Heart disease and stroke statistics-2011 update: a report from the American Heart Association," *Circulation*, vol. 123, pp. 18–209, 2011.

[4] *World Population Ageing 2009*, Department of Economic and Social Affairs of the United Nations, 2010.

[5] F. Alla, F. Zannad, and G. Filippatos, "Epidemiology of acute heart failure syndromes," *Heart Failure Reviews*, vol. 12, no. 2, pp. 91–95, 2007.

[6] C. Berry, D. R. Murdoch, and J. J. V. McMurray, "Economics of chronic heart failure," *European Journal of Heart Failure*, vol. 3, no. 3, pp. 283–291, 2001.

[7] A. Bundkirchen and R. H. G. Schwinger, "Epidemiology and economic burden of chronic heart failure," *European Heart Journal Supplements*, vol. 6, pp. 57–60, 2004.

[8] S. Stewart, "Financial aspects of heart failure programs of care," *European Journal of Heart Failure*, vol. 7, no. 3, pp. 423–428, 2005.

[9] J. S. Ross, J. Chen, Z. Lin et al., "Recent national trends in readmission rates after heart failure hospitalization," *Circulation: Heart Failure*, vol. 3, no. 1, pp. 97–103, 2010.

[10] S. Stewart, K. MacIntyre, D. J. Hole, S. Capewell, and J. J. McMurray, "More 'malignant' than cancer? Five-year survival following a first admission for heart failure," *European Journal of Heart Failure*, vol. 3, no. 3, pp. 315–322, 2001.

[11] F. A. McAlister, S. Stewart, S. Ferrua, and J. J. J. V. McMurray, "Multidisciplinary strategies for the management of heart failure patients at high risk for admission: a systematic review of randomized trials," *Journal of the American College of Cardiology*, vol. 44, no. 4, pp. 810–819, 2004.

[12] E. Seto, "Cost comparison between telemonitoring and usual care of heart failure: a systematic review," *Telemedicine and E-Health*, vol. 14, no. 7, pp. 679–686, 2008.

[13] C. Klersy, A. De Silvestri, G. Gabutti, F. Regoli, and A. Auricchio, "A meta-analysis of remote monitoring of heart failure patients," *Journal of the American College of Cardiology*, vol. 54, no. 18, pp. 1683–1694, 2009.

[14] S. C. Inglis, R. A. Clark, F. A. McAlister et al., "Structured telephone support or telemonitoring programmes for patients with chronic heart failure," *Cochrane Database of Systematic Reviews*, vol. 4, no. 8, Article ID CD007228, 2010.

[15] J. P. Riley and M. R. Cowie, "Telemonitoring in heart failure," *Heart and Education in Heart*, vol. 95, no. 23, pp. 1964–1968, 2009.

[16] G. van den Broek, F. Cavallo, and C. Wehrmann, "Ambient Assisted Living Roadmap," March 2010, http://www.aaliance.eu.

[17] S. J. Devaraj and K. Ezra, "Current trends and future challenges in wireless telemedicine system," in *Proceedings of the 3rd International Conference on Electronics Computer Technology (ICECT '11)*, vol. 4, pp. 417–421, April 2011.

[18] C. Fabbricatore, M. Zucker, S. Ziganki, and A. P. Karduck, "Towards an unified architecture for smart home and ambient assisted living solutions: a focus on elderly people," in *Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference (DEST '11)*, pp. 305–311, June 2011.

[19] A. J. Jara, M. A. Zamora, and A. F. G. Skarmeta, "An architecture for ambient assisted living and health environments," in *Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing, and Ambient Assisted Living*, vol. 5518 of *Lecture Notes in Computer Science*, pp. 882–889, 2009.

[20] J. H. Shin, B. Lee, and K. Suk Park, "Detection of abnormal living patterns for elderly living alone using support vector data description," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 3, pp. 438–448, 2011.

[21] Aerotel Medical System, http://www.aerotel.com.

[22] Advanced Digital Technologies, http://www.aditechsrl.com/.

[23] Parsys telemedicine, http://www.parsyssante.com/.

[24] Tunstall, http://www.tunstall.it/.

[25] Telcomed, http://www.telcomed.ie/.

[26] Insight Telehealth System, http://www.itsmyhealthyheart.com.

[27] K. Kang, K. J. Park, J. J. Song, C. H. Yoon, and L. Sha, "A medical-grade wireless architecture for remote electrocardiography," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 2, pp. 260–267, 2011.

[28] A. Gund, I. Ekman, K. Lindecrantz, B. A. Sjogvist, E. L. Staaf, and N. Thorneskold, "Design evaluation of a home-based telecare system for Chronic heart failure patients," in *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5851–5854, 2008.

[29] C. Masella, P. Zanaboni, G. Borghi, A. Castelli, M. Marzegalli, and C. Tridico, "Introduction of a telemonitoring service for patients affected by Chronic heart failure," in *Proceedings of the 11th IEEE International Conference on E-Health Networking, Applications and Services (Healthcom '09)*, pp. 138–145, December 2009.

[30] E. Villalba, D. Salvi, M. Ottaviano, I. Peinado, M. T. Arredondo, and A. Akay, "Wearable and mobile system to manage remotely heart failure," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 6, pp. 990–996, 2009.

[31] R. H. Dolin, L. Alschuler, S. Boyer et al., "HL7 clinical document architecture, release 2," *Journal of the American Medical Informatics Association*, vol. 13, no. 1, pp. 30–39, 2006.

[32] Implementation Guide for CDA Release 2.0 Personal Healthcare Monitoring Report (PHMR), http://www.hl7.org/.

[33] M. Yuksel and A. Dogac, "Interoperability of medical device information and the clinical applications: an HL7 RMIM based on the ISO/IEEE 11073 DIM," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 4, pp. 557–566, 2011.

[34] B. Shrestha, E. Hossain, and S. Camorlinga, "IEEE 802.15.4 MAC with GTS transmission for heterogeneous devices with application to wheelchair body-area sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 5, pp. 767–777, 2011.

[35] R. Trobec and I. Tomašić, "Synthesis of the 12-lead electrocardiogram from differential leads," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 4, pp. 615–621, 2011.

[36] L. Fanucci, S. Saponara, T. Bacchillone et al., "Sensing devices and sensor signal processing for remote monitoring of vital signs in CHF patients," *IEEE Transactions on Instrumentation and Measurement*, vol. 62, no. 3, pp. 553–569, 2013.

[37] J. Pan and W. J. Tompkins, "A real-time QRS detection algorithm," *IEEE Transactions on Biomedical Engineering*, vol. 32, no. 3, pp. 230–236, 1985.

[38] N. M. Arzeno, Z. D. Deng, and C. S. Poon, "Analysis of first-derivative based QRS detection algorithms," *IEEE Transactions on Biomedical Engineering*, vol. 55, no. 2, pp. 478–484, 2008.

[39] I. Sánchez-Tato, J. C. Senciales, J. Salinas et al., "Health @ home: a telecare system for patients with chronic heart failure," in *Proceedings of the 5th International Conference on Broadband and Biomedical Communications (IB2Com '10)*, pp. 1–5, December 2010.

[40] Spring development framework for JavaEE, http://www.springsource.org/.

[41] Systemized Nomenclature of Medicine—Clinical Terms, http://www.nlm.nih.gov/.

[42] Logical Observation Names and Identifier, http://loinc.org/.

[43] B.-K. Miller and W. MacCaull, "Toward Web-based Careflow management systems," *Journal of Emerging Technologies in Web Intelligence*, vol. 1, no. 2, pp. 137–145, 2009.

[44] B. Chen, L. A. Clarke, G. S. Avrunin, L. J. Osterweil, E. A. Henneman, and P. L. Henneman, "Analyzing medical processes," in *Proceedings of the 30th International Conference on Software Engineering (ICSE '08)*, pp. 623–632, 2008.

[45] L. Pecchia, P. Melillo, M. Sansone, and M. Bracale, "Discrimination power of short-term heart rate variability measures for CHF assessment," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 1, pp. 40–46, 2011.

Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2013, Article ID 710275, 26 pages
http://dx.doi.org/10.1155/2013/710275

Research Article

Untangling RFID Privacy Models

Iwen Coisel and Tania Martin

ICTEAM/Crypto Group and ICTEAM/GSI, Université Catholique de Louvain, 1348 Louvain-la-Neuve, Belgium

Correspondence should be addressed to Tania Martin; tania.martin@uclouvain.be

Received 25 May 2012; Accepted 24 July 2012

Academic Editor: Agusti Solanas

The rise of wireless applications based on RFID has brought up major concerns on privacy. Indeed nowadays, when such an application is deployed, informed customers yearn for guarantees that their privacy will not be threatened. One formal way to perform this task is to assess the privacy level of the RFID application with a model. However, if the chosen model does not reflect the assumptions and requirements of the analyzed application, it may misevaluate its privacy level. Therefore, selecting the most appropriate model among all the existing ones is not an easy task. This paper investigates the eight most well-known RFID privacy models and thoroughly examines their advantages and drawbacks in three steps. Firstly, five RFID authentication protocols are analyzed with these models. This discloses a main worry: although these protocols intuitively ensure different privacy levels, no model is able to accurately distinguish them. Secondly, these models are grouped according to their features (e.g., tag corruption ability). This classification reveals the most appropriate candidate model(s) to be used for a privacy analysis when one of these features is especially required. Furthermore, it points out that none of the models are comprehensive. Hence, some combinations of features may not match any model. Finally, the privacy properties of the eight models are compared in order to provide an overall view of their relations. This part highlights that no model globally outclasses the other ones. Considering the required properties of an application, the thorough study provided in this paper aims to assist system designers to choose the best suited model.

1. Introduction

Radio Frequency IDentification (RFID) is a technology that permits identifying and authenticating remote objects or persons without line of sight. In a simple manner, a tag (i.e., a transponder composed of a microcircuit and an antenna) is embedded into an object and interacts with a reader when it enters within its electromagnetic field. The first use of RFID goes back to the early 1940s, during World War II, when the Royal Air Force deployed the IFF (Identify Friend or Foe) system to identify the Allies airplanes. Today, RFID is more and more exploited in many domains such as library management, pet identification, antitheft cars, anticounterfeiting, ticketing in public transportation, access control, or even biometric passports. It thus covers a wide ranging of wireless technologies, from systems based on low-cost tags (such as EPCs [1]) to more evolved ones operating with contactless smartcards [2, 3].

As predictable, some problems come up with this large-scale deployment. One general assumption of RFID systems is that the messages exchanged between the tags and the readers can easily be eavesdropped by an adversary. This raises the problem of information disclosure when the data emitted by a tag reveal details about its holder (called "information leakage"), but also when the eavesdropping of communications allows tracking a tag at different places or times (called "malicious traceability") and consequently its holder. Many articles pointed out the dangers of RFID with respect to privacy, and the authorities are now aware of this problem. For instance, Ontario Information and Privacy Commissioner Cavoukian aims to advocate the concept of "privacy-by-design" [4] which states that privacy should be put in place in every IT system before its widespread use. In 2009, the European Commissioner for Justice, Fundamental Rights and Citizenship issued a recommendation [5] which strongly supports the implementation of privacy in RFID-based applications.

Various researches have emerged these last years to fight against information leakage and malicious traceability in RFID. However, the search for a generic, efficient, and

secure solution that can be implemented in reasonably costly tags remains open [6–8]. Solutions are usually designed empirically and analyzed with ad hoc methods that do not detect all their weaknesses. In parallel, many investigations have been conducted to formalize the privacy notion in RFID. In 2005, Avoine was the earliest researcher to present a privacy model [9]. Since then, many attempts [10–22] have been carried out to propose a convenient and appropriate privacy model for RFID. But each one suffers from distinct shortcomings. In particular, most of these models generally do not take into account all the alternatives that a power may offer to an adversary. For instance, when an adversary is allowed to corrupt a tag, then several possibilities may arise: a corrupted tag could be either destroyed or not, and, in the last case, this tag could still be requested to interact within the system. At Asiacrypt 2007, Vaudenay introduced the most evolved RFID privacy model [22] known so far. However, this model is not as convenient as some protocol designers may expect, and they sometimes prefer to use a less comprehensive model to analyze a system. Consequently, providing an analysis and a comparison of the major RFID privacy models is meaningful to help designers in their choice. Such a work aims to highlight the strengths and weaknesses of each model. Su et al. already achieved a similar work in [23]. Unfortunately, they only focused on privacy notions and did not consider all the subtleties that are brought by different models. As a consequence, their study considers some models as weak, even though they offer interesting properties.

Our contribution is threefold. Firstly, in Sections 3 to 10, we chronologically present eight well-known models designed to analyze identification/authentication protocols preserving privacy. Some of them are very popular like [9, 16, 22]. Other ones have interesting frameworks like [12, 13, 18] (e.g., [18] is derived from the well-known universal composability framework). Other alternative models are attractive successors of [22], such as [11, 15]. Secondly, in Section 11, we analyze five different authentication protocols with each of these models in order to exhibit the lack of granularity of the state of the art. Finally, in Sections 12 and 13, we thoroughly compare the eight models regarding their different features and their privacy notions. We show that none of these models can fairly analyze and compare protocols. This fact is especially undeniable when the system's assumptions (that can differ from one system to another) are taken into account for an analysis.

2. Common Definitions

In this section, we give all the common definitions that are used in the presented privacy models.

2.1. The RFID System. For all the privacy models, an RFID system $\mathcal{S}$ is composed of three kinds of entities: tags, readers, and a centralized database. It is generally considered that the database and the readers are connected online all together through a secure channel, and therefore they form one unique entity, the reader.

We denote $\mathcal{T}$ as a tag, $\mathcal{R}$ as the reader, and DB as the reader's database. A tag $\mathcal{T}$ is able to communicate with $\mathcal{R}$ when it enters into $\mathcal{R}$'s electromagnetic field. Then both reader and tag can participate together to an RFID protocol execution π. This protocol can be an identification or an authentication protocol. We define an i-pass RFID protocol as being a protocol where i messages are exchanged between $\mathcal{R}$ and $\mathcal{T}$.

The reader $\mathcal{R}$ is a powerful transceiver device whose computation capabilities approach the ones of a small computer. A tag $\mathcal{T}$ is a transponder with identifier $\mathsf{ID}_{\mathcal{T}}$. Its memory can vary from a hundred of bits (as for EPC tags [1]) to a few Kbytes (such as contactless smartcards [2, 3]). Its computation capabilities are generally much lower than a reader, but, depending on the tag, it can perform simple logic operations, symmetric-key cryptography, or even public-key cryptography. A tag is considered as *legitimate* when it is registered in the database DB as being an authorized entity of the system. The database DB stores, at least, the identifier $\mathsf{ID}_{\mathcal{T}}$ and potentially a secret $\mathsf{k}_{\mathcal{T}}$ of each legitimate tag $\mathcal{T}$ involved in the system.

2.2. Basic Definitions. First, we define λ as the security parameter of the system $\mathcal{S}$ and poly(·) as a polynomial function. Thus, we define $\varepsilon(\lambda) : \mathbb{N} \to \mathbb{R}$ as being a negligible function in λ if, for every positive function poly(·), there exists an integer N such that, for all $\lambda > N$, $|\varepsilon(\lambda)| < 1/\text{poly}(\lambda)$.

Then, we define all the different entities that may play a role in the presented privacy models. An *adversary* $\mathcal{A}$ is a malicious entity whose aim is to perform some attacks, either through the wireless communications between readers and tags (e.g., eavesdropping), or on the RFID devices themselves (e.g., corruption of a device and obtaining all the information stored on it). The adversary advantage is the success measure of an attack performed by $\mathcal{A}$. In some models, $\mathcal{A}$ is requested to answer to a kind of riddle, which is determined by an honest entity, called *challenger* $\mathcal{C}$. A *challenge tag* is a tag which is suffering from an attack performed by $\mathcal{A}$. It can be chosen either by $\mathcal{A}$ or by $\mathcal{C}$.

Generally, a modelization with oracles is used to represent the possible interactions between $\mathcal{A}$ and the system. Thus, $\mathcal{A}$ carries out its attack on the system, performing some queries to the oracles that simulate the system. The generic oracles used in the presented privacy models are detailed in Section 2.4.

We consider that $\mathcal{A}$ is able to play/interact with a tag when this last one is in $\mathcal{A}$'s neighborhood. At that moment, the tag is called by its pseudonym $\mathcal{T}$ (not by its identifier $\mathsf{ID}_{\mathcal{T}}$). During an attack, if a tag goes out and comes back to $\mathcal{A}$'s neighborhood, then it is considered that its pseudonym has changed. This notion is detailed in the Vaudenay model [22] (see Section 5). The same case happens when a set of tags is given to the challenger $\mathcal{C}$: when $\mathcal{C}$ gives the tags back to $\mathcal{A}$, their pseudonyms are changed.

2.3. Procedures. Most of the models studied in this paper focus on an RFID system $\mathcal{S}$ based on an anonymous identification protocol implying a single reader and several tags.

The system is generally composed of several procedures, either defining how to set up the system, the reader, and the tags, or defining the studied protocol. One way to define these procedures is detailed in the following. Note that this is just a generalization but it may be different in some models.

(i) $\mathsf{SetupReader}(1^\lambda)$ defines $\mathcal{R}$'s parameters (e.g., generating a private/public key pair $(\mathsf{K_S}, \mathsf{K_P})$) depending on the security parameter λ. It also creates an empty database DB which will later contain, at least, the identifiers and secrets of all tags.

(ii) $\mathsf{SetupTag}_{\mathsf{K_P}}(\mathsf{ID}_\mathcal{T})$ returns $\mathsf{k}_\mathcal{T}$, that is, the secret $\mathsf{k}_\mathcal{T}$ of the tag $\mathcal{T}$ with identifier $\mathsf{ID}_\mathcal{T}$. $(\mathsf{ID}_\mathcal{T}, \mathsf{k}_\mathcal{T})$ is stored in the database DB of the reader.

(iii) Ident is a polynomial-time interactive protocol between the reader $\mathcal{R}$ and a tag $\mathcal{T}$, where $\mathcal{R}$ ends with a private tape Output. At the end of the protocol, the reader either accepts the tag (if legitimate) and $\mathsf{Output} = \mathsf{ID}_\mathcal{T}$, or rejects it (if not) and $\mathsf{Output} = \perp$.

2.4. The Generic Oracles. An adversary $\mathcal{A}$ is able to interact/play with the system with the following oracles. First, it can setup a new tag of identifier $\mathsf{ID}_\mathcal{T}$.

(i) $\textsc{CreateTag}(\mathsf{ID}_\mathcal{T})$ creates a tag $\mathcal{T}$ with a unique identifier $\mathsf{ID}_\mathcal{T}$. It uses $\mathsf{SetupTag}_{\mathsf{K_P}}$ to set up the tag. It updates DB, adding this new tag.

$\mathcal{A}$ can ask for a full execution of the protocol on a tag $\mathcal{T}$.

(i) $\textsc{Execute}(\mathcal{T}) \rightarrow (\pi, \mathsf{transcript})$ executes an Ident protocol between $\mathcal{R}$ and $\mathcal{T}$. It outputs the transcript of the protocol execution π, that is the whole list of the successive messages of the execution π.

Also, it can decompose a protocol execution, combining the following oracles.

(i) $\textsc{Launch}() \rightarrow \pi$ makes $\mathcal{R}$ start a new Ident protocol execution π.

(ii) $\textsc{SendReader}(m, \pi) \rightarrow r$ sends a message m to $\mathcal{R}$ in the protocol execution π. It outputs the response r of the reader.

(iii) $\textsc{SendTag}(m, \mathcal{T}) \rightarrow r$ sends a message m to $\mathcal{T}$. It outputs the response r of the tag.

Then, $\mathcal{A}$ can obtain for the reader's result of a protocol execution π.

(i) $\textsc{Result}(\pi) \rightarrow x$: when π is completed, it outputs $x = 1$ if $\mathsf{Output} \neq \perp$, and $x = 0$ otherwise.

And finally, it can corrupt a tag $\mathcal{T}$ in order to recover its secret.

(i) $\textsc{Corrupt}(\mathcal{T}) \rightarrow \mathsf{k}_\mathcal{T}$ returns the current secret $\mathsf{k}_\mathcal{T}$ of $\mathcal{T}$.

If the conditions of the oracles' uses are not respected, then the oracles return $\perp$. Note that these definitions are generic ones. Some models do not use exactly the same generic oracles: in those cases, some refinements will be provided on their definitions.

3. Avoine [9], 2005

In 2005, Avoine proposed the first privacy model for RFID systems. The goal was to analyze the untraceability notion of 3-pass protocols following the idea of communication intervals: the adversary $\mathcal{A}$ asks some oracles' queries on specific intervals of the targeted tags lives. The privacy notion behind this model represents the unfeasibility to distinguish one tag among two.

3.1. The Oracles. This model considers that each tag has a unique and independent secret, and that, at the initialization of the system, DB already stores all the tags' secrets, that is, a SetupTag has already been performed on every tag.

Then $\mathcal{A}$ has only access to the following modified generic oracles adapted for 3-pass protocols. Instead of using the entities' names, Avoine uses the protocol executions names. Since $\mathcal{T}$ and $\mathcal{R}$ can run several protocol executions, $\pi^i_\mathcal{T}$ (resp., $\pi^j_\mathcal{R}$) denotes the ith (resp., jth) execution of $\mathcal{T}$ (resp., $\mathcal{R}$). These notations favor the precise description of $\mathcal{R}$'s and $\mathcal{T}$'s lifetimes.

(i) $\textsc{SendTag}(m_1, m_3, \pi^i_\mathcal{T}) \rightarrow r$ sends a request m_1 to $\mathcal{T}$, and then $\mathcal{A}$ sends the message m_3 after receiving $\mathcal{T}$'s answer r. This is done during the execution $\pi^i_\mathcal{T}$ of $\mathcal{T}$.

(ii) $\textsc{SendReader}(m_2, \pi^j_\mathcal{R}) \rightarrow r$ sends the message m_2 to $\mathcal{R}$ in the protocol execution $\pi^j_\mathcal{R}$. It outputs $\mathcal{R}$'s answer r.

(iii) $\textsc{Execute}(\pi^i_\mathcal{T}, \pi^j_\mathcal{R}) \rightarrow \mathsf{transcript}$ executes a whole execution of the protocol between $\mathcal{T}$ and $\mathcal{R}$. This is done during the execution $\pi^i_\mathcal{T}$ of $\mathcal{T}$ and the execution $\pi^j_\mathcal{R}$ of $\mathcal{R}$. $\mathcal{A}$ obtains the whole transcript.

(iv) $\textsc{Execute}^*(\pi^i_\mathcal{T}, \pi^j_\mathcal{R}) \rightarrow \mathcal{R}$-transcript this is the same as the normal Execute. But it only returns the $\mathcal{R}$-transcript, that is, the messages sent by $\mathcal{R}$.

(v) $\textsc{Corrupt}(\pi^i_\mathcal{T}) \rightarrow \mathsf{k}_\mathcal{T}$: returns the current secret $\mathsf{k}_\mathcal{T}$ of $\mathcal{T}$ when the tag is in its ith execution.

The goal of the $\textsc{Execute}^*$ oracle is to simulate the fact that the forward channel (from reader to tag) has a longer communication range than the backward channel (from tag to reader) and therefore can be easily eavesdropped. It formalizes the asymmetry regarding the channels.

Two remarks are of interest for the Corrupt oracle. First, Corrupt can be used only once by $\mathcal{A}$. After this oracle query, $\mathcal{A}$ cannot use the other oracles anymore. Second, Corrupt is called on the tag execution number, and not the tag itself. This allows $\mathcal{A}$ to specify exactly the targeted moment of the tag's life.

During its attack, $\mathcal{A}$ has access to the oracles $\mathcal{O} \subset \{T, R, E, E^*, C\} = \{\textsc{SendTag}, \textsc{SendReader}, \textsc{Execute}, \textsc{Execute}^*, \textsc{Corrupt}\}$.

Avoine denotes $\omega_i(\mathcal{T})$ as being the result of an oracle query on $\mathcal{T}$: therefore $\omega_i(\mathcal{T}) \in \{\textsc{SendTag}(*, *, \pi^i_\mathcal{T}), \textsc{Execute}(\pi^i_\mathcal{T}, *), \textsc{Execute}^*(\pi^i_\mathcal{T}, *), \textsc{Corrupt}(\pi^i_\mathcal{T})\}$. Avoine defines an *interaction* $\Omega_I(\mathcal{T})$ as being a set of executions on

the same tag $\mathcal{T}$ during an interval I when $\mathcal{A}$ can play with $\mathcal{T}$. Formally, $\Omega_I(\mathcal{T}) = \{\omega_i(\mathcal{T}) \mid i \in I\} \cup \{\text{SendReader}(*, \pi_*^j) \mid j \in J\}$, where $I, J \subset \mathbb{N}$. By this definition, the length of $\Omega_I(\mathcal{T})$ is $|I|$.

Avoine also defines a function *Oracle* which takes as parameters a tag $\mathcal{T}$, an interval I, and the oracles $\mathcal{O}$, and which outputs the interaction $\widehat{\Omega_I}(\mathcal{T})$ that maximizes $\mathcal{A}$'s advantage.

3.2. Untraceability Experiments. Avoine defines two experiments to represent two untraceability notions. They depend on λ_{ref} and λ_{chal}, which represent, respectively, a reference length and a challenge length and which are function of the security parameter λ.

The first experiment given in Box 1 works as follows. First, $\mathcal{A}$ receives the interactions of a tag $\mathcal{T}$ during an interval I that it chooses. Then, it receives the interactions of the challenge tags $\mathcal{T}_0$ and $\mathcal{T}_1$, also during the intervals I_0 and I_1 that it chooses, such that $\mathcal{T} = \mathcal{T}_0$ or $\mathcal{T}_1$. This last information is unknown to $\mathcal{A}$. Additionally here, none of these two intervals I_0 and I_1 cross the interval I of $\mathcal{T}$. At the end, $\mathcal{A}$ has to decide which one of the challenge tags is the tag $\mathcal{T}$.

The second experiment given in Box 2 has the same mechanism. The only difference is that, now, $\mathcal{C}$ is the one that chooses the intervals I_0 and I_1 of the challenge tags, and not $\mathcal{A}$ anymore.

3.3. Untraceability Notions. From the experiments defined above, the notions of Existential-UNT and Universal-UNT are extended in this model, depending on restrictions about the choices of I_0 and I_1. Existential-UNT is when $\mathcal{A}$ chooses I_0 and I_1, whereas Universal-UNT is when $\mathcal{C}$ chooses them. Then, if $I < I_0, I_1$ (resp., $I > I_0, I_1$), that means I_0 and I_1 take place after (resp., before) I, with respect to the lifetime of the system.

(i) If $\mathcal{A}$ (resp., $\mathcal{C}$) chooses I_0 and I_1 such that $I < I_0, I_1$, then it is denoted Existential$^+$ (resp., Universal$^+$).

(ii) If $\mathcal{A}$ (resp., $\mathcal{C}$) chooses I_0 and I_1 such that $I > I_0, I_1$, then it is denoted Existential$^-$ (resp., Universal$^-$).

The notion of Universal$^-$ when the Corrupt oracle is used is called Forward-UNT.

Definition 1 (untraceability [9]). An RFID system $\mathcal{S}$ is said to be P-UNT-$\mathcal{O}$ (for $P \in \{\text{Existential}, \text{Forward}, \text{Universal}\}$) if, for every adversary $\mathcal{A}$,

$$\left|\Pr\left(\text{Exp}_{\mathcal{S},\mathcal{A}}^{P\text{-UNT}}[\lambda_{\text{ref}}, \lambda_{\text{chal}}, \mathcal{O}] \text{ succeeds}\right) - \frac{1}{2}\right| \leq \varepsilon(\lambda_{\text{ref}}, \lambda_{\text{chal}}). \tag{1}$$

Direct implications are made from these notions:

$$\boxed{\text{Existential-UNT-}\mathcal{O} \Longrightarrow \text{Forward-UNT-}\mathcal{O} \Longrightarrow \text{Universal-UNT-}\mathcal{O}} \tag{2}$$

4. Juels and Weis [16], 2007

Two years after Avoine's publication, Juels and Weis proposed a new privacy model, referred in the sequel as JW, based on indistinguishability of tags. It intended to analyze classical challenge/response protocols based on symmetric-key cryptography (with possible additional messages in order to update the tags keys).

In their article, the authors highlighted that the Avoine model lacks two important features. Firstly, they proved that it is unable to catch an important attack on systems where tags have correlated secrets, because Avoine's adversary can only play with two tags. Secondly, they showed that Avoine did not have hindsight regarding all the possible attacks that can be performed on a protocol. The Avoine model does not capture all the relevant information that can be extracted from a protocol execution. For instance, it does not consider that $\mathcal{A}$ has access to any execution result. However, this simple "side information bit" allows formalizing a special kind of attacks on desynchronizable protocols like OSK, as explained in Appendix B.3. and in [24]. Therefore, the JW model aimed to fill that gap.

4.1. Oracles. At the initialization of the system, DB already stores all the tags' content, that is, a SetupTag has already been performed on every tag. Then $\mathcal{A}$ has access to the generic oracles Launch SendTag and SendReader, with the difference that the Output of SendReader includes the output of Result. It has furthermore access to the following oracles.

(i) $\text{TagInit}(\mathcal{T}) \rightarrow \pi$: when $\mathcal{T}$ receives this query, it begins a new protocol execution π and deletes the information related to any existing execution.

(ii) $\text{SetKey}(\mathcal{T}, \mathsf{k}_{\mathcal{T}}^{\text{new}}) \rightarrow \mathsf{k}_{\mathcal{T}}$: when $\mathcal{T}$ receives this query, it outputs its current key $\mathsf{k}_{\mathcal{T}}$ and replaces it by a new one, $\mathsf{k}_{\mathcal{T}}^{\text{new}}$.

The SetKey oracle is equivalent to the Corrupt oracle given in Section 2.4 in the sense that it reveals to $\mathcal{A}$ the tag's current key. Note that its use and its result have an interesting feature: $\mathcal{A}$ is able to put any new key in the targeted tag: either the revealed one or a random one (that can be illegitimate).

4.2. Privacy Experiment. Let ρ, σ, and τ be, respectively, the numbers of Launch, computation steps (represented by the SendReader and SendTag queries), and TagInit that are allowed to $\mathcal{A}$. Let n be the total number of tags involved in the system $\mathcal{S}$. The privacy experiment is given in Box 3.

4.3. Privacy Notions. From the previous experiment, the JW model defines the following privacy property, where ρ, σ, and τ can be function of the system security parameter λ.

Experiment $\mathrm{Exp}^{\text{Existential-UNT}}_{\mathcal{S},\mathcal{A}}[\lambda_{\text{ref}}, \lambda_{\text{chal}}, \mathcal{O}]$.

(1) $\mathscr{C}$ initializes the system $\mathcal{S}$.
(2) $\mathcal{A}$ requests $\mathscr{C}$ to receive a tag $\mathcal{T}$.
(3) $\mathcal{A}$ chooses I, queries *Oracle* $(\mathcal{T}, I, \mathcal{O})$ where $|I| \leq \lambda_{\text{ref}}$, and then receives $\widehat{\Omega_I}(\mathcal{T})$.
(4) $\mathcal{A}$ requests $\mathscr{C}$ to receive two challenge tags $\mathcal{T}_0$ and $\mathcal{T}_1$, such that $\mathcal{T} = \mathcal{T}_0$ or $\mathcal{T}_1$.
(5) $\mathcal{A}$ chooses I_0 and I_1 such that $|I_0| \leq \lambda_{\text{chal}}$, $|I_1| \leq \lambda_{\text{chal}}$, and $(I_0 \cup I_1) \cap I = \varnothing$.
(6) $\mathcal{A}$ queries *Oracle* $(\mathcal{T}_0, I_0, \mathcal{O})$ and *Oracle* $(\mathcal{T}_1, I_1, \mathcal{O})$, and then receives $\widehat{\Omega_{I_0}}(\mathcal{T}_0)$ and $\widehat{\Omega_{I_1}}(\mathcal{T}_1)$.
(7) $\mathcal{A}$ decides which of $\mathcal{T}_0$ or $\mathcal{T}_1$ is $\mathcal{T}$, and outputs a guess bit b.
$\mathrm{Exp}^{\text{Existential-UNT}}_{\mathcal{S},\mathcal{A}}$ succeeds if $\mathcal{T} = \mathcal{T}_b$.

Box 1

Experiment $\mathrm{Exp}^{\text{Universal-UNT}}_{\mathcal{S},\mathcal{A}}[\lambda_{\text{ref}}, \lambda_{\text{chal}}, \mathcal{O}]$

(1) $\mathscr{C}$ initializes the system $\mathcal{S}$.
(2) $\mathcal{A}$ requests $\mathscr{C}$ to receive a tag $\mathcal{T}$.
(3) $\mathcal{A}$ chooses I, queries *Oracle* $(\mathcal{T}, I, \mathcal{O})$ where $|I| \leq \lambda_{\text{ref}}$, and then receives $\widehat{\Omega_I}(\mathcal{T})$. Here I is known by $\mathscr{C}$.
(4) $\mathcal{A}$requests $\mathscr{C}$ to receive two challenges $\mathcal{T}_0$, $\mathcal{T}_1$, I_0 and I_1, such that $\mathcal{T} = \mathcal{T}_0$ or $\mathcal{T}_1$.
(5) $\mathcal{A}$ queries *Oracle* $(\mathcal{T}_0, I_0, \mathcal{O})$ and *Oracle* $(\mathcal{T}_1, I_1, \mathcal{O})$, and then receives $\widehat{\Omega_{I_0}}(\mathcal{T}_0)$ and $\widehat{\Omega_{I_1}}(\mathcal{T}_1)$.
(6) $\mathcal{A}$ decides which of $\mathcal{T}_0$ or $\mathcal{T}_1$ is $\mathcal{T}$, and outputs a guess bit b.
$\mathrm{Exp}^{\text{Universal-UNT}}_{\mathcal{S},\mathcal{A}}$ succeeds if $\mathcal{T} = \mathcal{T}_b$.

Box 2

Definition 2 ((ρ, σ, τ)-privacy [16]). A protocol initiated by $\mathcal{R}$ in an RFID system $\mathcal{S}$ with security parameter λ is (ρ, σ, τ)-*private* if, for every adversary $\mathcal{A}$,

$$\left|\Pr\left(\mathrm{Exp}^{\text{JW-priv}}_{\mathcal{S},\mathcal{A}}[\lambda, n, \rho, \sigma, \tau] \text{ succeeds}\right) - \frac{1}{2}\right| \leq \varepsilon(\lambda). \quad (3)$$

Considering a variant of experiment $\mathrm{Exp}^{\text{JW-priv}}_{\mathcal{S},\mathcal{A}}$ where the "*except* $\mathcal{T}_b^*$" is removed from step (6.b), then forward-(ρ, σ, τ)-privacy can be defined in the same way as the previous definition.

Note that, if $\mathcal{A}$ uses SetKey to put an illegitimate key in a tag, then this last one will possibly no longer be authenticated successfully by the reader. Nevertheless, whether this is performed on the nonchallenge tags or on $\mathcal{T}_b^*$ (only for the forward-(ρ, σ, τ)-privacy experiment), this does not help $\mathcal{A}$ to find more easily the bit b and thus does not influence its success to win the experiment.

5. Vaudenay [22], 2007

Later the same year, Vaudenay proposed formal definitions for RFID systems and adversaries and considered that a system $\mathcal{S}$ can be characterized by two notions: security and privacy. In this paper, we only present the privacy notion. Vaudenay's article followed some joint work done with Bocchetti [25], and its goal was to propose a comprehensive model that can formalize a wide range of adversaries. This characteristic is missing in the previous models and turns to be an asset of the Vaudenay model.

This model defines tags with respect to the adversary possibility to interact with them, as explained in Section 2.2. Clearly, when a tag is within $\mathcal{A}$'s neighborhood, it is said to be drawn and has a pseudonym so that $\mathcal{A}$ is able to communicate with the tag. In the opposite situation, a tag is said to be free (i.e., not drawn), and $\mathcal{A}$ cannot communicate with it. Consequently, the model considers that, at any given time, a tag can be either free or drawn. For example, the same tag with identifier $\mathsf{ID}_{\mathcal{T}}$ which is drawn, freed, and drawn again has two pseudonyms: $\mathcal{A}$ sees two different tags. Additionally, all the tags may not be accessible to $\mathcal{A}$ during all the attack: for instance, $\mathcal{A}$ may only play with two (drawn) tags during its attack.

5.1. Oracles. Contrary to the other previous models, DB is empty at the initialization of the system. Then $\mathcal{A}$ has access to all the generic oracles defined in Section 2.4. The only modification done on these ones is that $\mathcal{A}$ can create a fake tag with CreateTag. In that case, no information related to this tag is stored in DB. It can also query the following ones.

(i) DrawTag(distr) $\rightarrow$ $(\mathcal{T}_1, b_1, \ldots, \mathcal{T}_k, b_k)$: following the distribution probability distr (which is specified by a polynomially bounded sampling algorithm), it randomly selects k tags between all the existing (not already drawn) ones. For each chosen tag, the oracle assigns to it a new pseudonym, denoted $\mathcal{T}_i$, and changes its status from free to drawn. Finally, the oracle outputs all the generated temporary tags $(\mathcal{T}_1, \ldots, \mathcal{T}_k)$ in any random order. If there is not

Experiment $\mathrm{Exp}^{\mathsf{JW\text{-}priv}}_{\mathcal{S},\mathcal{A}}[\lambda, n, \rho, \sigma, \tau]$

Setup:
(1) $\mathscr{C}$ initializes the system $\mathcal{S}$.
Phase 1 (Learning):
(2) $\mathscr{A}$ may do the following in any interleaved order:
  (a) Make Launch and TagInit queries, without exceeding ρ and τ overall queries respectively.
  (b) Make arbitrary SetKey queries to any $(n-2)$ tags.
  (c) Make SendReader and SendTag queries, without exceeding σ overall queries.
Phase 2 (Challenge):
(3) $\mathscr{A}$ selects two challenge tags $\mathcal{T}_i$ and $\mathcal{T}_j$ to which it did not send SetKey queries.
(4) Let $\mathcal{T}_0^* = \mathcal{T}_i$ and $\mathcal{T}_1^* = \mathcal{T}_j$, and remove both from the current tag set.
(5) $\mathscr{C}$ chooses a bit b at random, and provides $\mathscr{A}$ access to $\mathcal{T}_b^*$.
(6) $\mathscr{A}$ may do the following in any interleaved order:
  (a) Make Launch and TagInit queries, without exceeding ρ and τ overall queries respectively.
  (b) Make arbitrary SetKey queries to any tag in the current tag set, *except* $\mathcal{T}_b^*$.
  (c) Make SendReader and SendTag queries, without exceeding σ overall queries.
(7) $\mathscr{A}$ outputs a guess bit b'.
$\mathrm{Exp}^{\mathsf{JW\text{-}priv}}_{\mathcal{S},\mathcal{A}}$ succeeds if $b = b'$.

Box 3

enough free tags (i.e., less than k), or tags already drawn, then the oracle outputs $\perp$. It is further assumed that this oracle returns bits $(b_1, \ldots, b_k)$ telling if each of the drawn tags is legitimate or not. All relations $(\mathcal{T}_i, \mathsf{ID}_{\mathcal{T}_i})$ are kept in an *a priori* secret table denoted Tab.

(ii) Free($\mathcal{T}$) moves the tag $\mathcal{T}$ from the status drawn to the status free. $\mathcal{T}$ is unavailable from now on.

5.2. Privacy Experiment. From the oracles given above, Vaudenay defines five classes of polynomial-time adversary, characterized by $\mathscr{A}$'s ability to use the oracles.

Definition 3 (adversary class [22]). An adversary class is said to be

(i) STRONG if $\mathscr{A}$ has access to all the oracles;

(ii) DESTRUCTIVE if $\mathscr{A}$ cannot use anymore a "corrupted" tag (i.e., the tag has been destroyed);

(iii) FORWARD if $\mathscr{A}$ can only use the Corrupt oracle after its first query to the Corrupt oracle;

(iv) WEAK if $\mathscr{A}$ has no access to the Corrupt oracle;

(v) NARROW if $\mathscr{A}$ has no access to the Result oracle.

Remark 4. The following relation is clear: WEAK $\subseteq$ FORWARD $\subseteq$ DESTRUCTIVE $\subseteq$ STRONG.

Note that the WIDE notion is the contrary to the NARROW one. If an adversary $\mathscr{A}$ is not said to be NARROW, then nothing is said, but the term WIDE is implicitly meant.

Vaudenay's privacy experiment is given in Box 4. P is the adversary class, $P \in \{\varnothing, \mathsf{NARROW}\} \times \{\mathsf{WEAK}, \mathsf{FORWARD}, \mathsf{DESTRUCTIVE}, \mathsf{STRONG}\}$.

5.3. Privacy Notions. To define the privacy property of Vaudenay, it is first needed to define the notions of *blinder* (i.e., an algorithm able to simulate the answers of some specific oracles) and *trivial adversary* (i.e., an adversary that learns nothing about the system).

Definition 5 (blinder, trivial adversary [22]). A blinder $\mathscr{B}$ for an adversary $\mathscr{A}$ is a polynomial-time algorithm which sees the same messages as $\mathscr{A}$ and simulates the Launch, SendReader, SendTag, and Result oracles to $\mathscr{A}$. $\mathscr{B}$ does not have access to the reader tapes, so it does not know the secret key nor the database.

A blinded adversary $\mathscr{A}^{\mathscr{B}}$ is itself an adversary that does not use the Launch, SendReader, SendTag, and Result oracles.

An adversary $\mathscr{A}$ is trivial if there exists a blinder $\mathscr{B}$ such that

$$\left|\Pr\left(\mathrm{Exp}^{\mathsf{Vaud\text{-}priv}}_{\mathcal{S},\mathcal{A}}[\lambda] \text{ succeeds}\right) - \Pr\left(\mathrm{Exp}^{\mathsf{Vaud\text{-}priv}}_{\mathcal{S},\mathcal{A}^{\mathscr{B}}}[\lambda] \text{ succeeds}\right)\right| \leq \varepsilon(\lambda)\,. \tag{4}$$

Definition 6 (privacy [22]). The RFID system $\mathcal{S}$ is said to be *P-private* if all the adversaries which belong to class P are trivial following Definition 5.

The implications between Vaudenay's privacy notions are as follows:

Experiment $\mathrm{Exp}^{\mathsf{Vaud\text{-}priv}}_{\mathcal{S},\mathcal{A}}[\lambda]$

(1) $\mathcal{C}$ initializes the system and sends 1^{λ}, and $\mathsf{K_p}$ to $\mathcal{A}$.
(2) $\mathcal{A}$ interacts with the whole system, limited by its class P.
(3) $\mathcal{A}$ analyzes the system without oracle queries.
(4) $\mathcal{A}$ receives the hidden table Tab of the DrawTag oracle.
(5) $\mathcal{A}$ returns *true* or *false*.
$\mathrm{Exp}^{\mathsf{Vaud\text{-}priv}}_{\mathcal{S},\mathcal{A}}$ succeeds if $\mathcal{A}$ returns *true*.

Box 4

$$\begin{array}{ccccccc} \mathsf{STRONG} & \Longrightarrow & \mathsf{DESTRUCTIVE} & \Longrightarrow & \mathsf{FORWARD} & \Longrightarrow & \mathsf{WEAK} \\ \Downarrow & & \Downarrow & & \Downarrow & & \Downarrow \\ \mathsf{NARROW\text{-}STRONG} & \Longrightarrow & \mathsf{NARROW\text{-}DESTRUCTIVE} & \Longrightarrow & \mathsf{NARROW\text{-}FORWARD} & \Longrightarrow & \mathsf{NARROW\text{-}WEAK} \end{array} \quad (5)$$

The main result of Vaudenay is that STRONG-privacy is impossible, by proving that a DESTRUCTIVE-private protocol is not NARROW-STRONG-private. However, Vaudenay does not define which privacy level should be targeted by a protocol: it is never specified if NARROW-STRONG-privacy is better or not than DESTRUCTIVE-privacy.

Also, it is not explicit how the blinded adversary $\mathcal{A}^{\mathcal{B}}$ operates. Basically, there are two options: (i) $\mathcal{A}^{\mathcal{B}}$ aims the same probability than $\mathcal{A}$, or (ii) $\mathcal{A}^{\mathcal{B}}$ aims the same behavior than $\mathcal{A}$. It is obvious that the first option allows proving the privacy of some protocols which are actually not private, but this should be correctly formalized.

5.4. Extensions of the Model

5.4.1. Model [21], 2008. Paise and Vaudenay extended the Vaudenay model to analyze mutual authentication protocols. Actually, they enriched the definition of the RFID system $\mathcal{S}$ by introducing an output on the tag side: either the tag accepts the reader (if legitimate) and outputs OK, or rejects it (if not) and outputs $\perp$. This formalizes the concept of *reader authentication*. Nevertheless, their extension does not modify the core of the Vaudenay model.

They also showed an important impossibility result: if the corruption of a tag reveals its entire state (and not only its secret $\mathsf{k}_{\mathcal{T}}$), then no RFID scheme providing reader authentication is NARROW-FORWARD-private. To counter this issue, they claimed that the temporary memory of a tag should be automatically erased as soon as the tag is put back as free. However, this idea is not formalized in the paper.

This division between the persistent and the temporary memory of a tag has also been investigated by Armknecht et al. [26]. Based on the work of Paise and Vaudenay, they showed several impossibility results in attack scenarios with special uses of tag corruption.

5.4.2. Model [20], 2011. Ouafi presented in his thesis an adaptation of the Vaudenay model in order to counterVaudenay's impossibility result of STRONG-privacy. Concretely, the author proposed to incorporate the blinder with the adversary, so that the blinder has the knowledge of all the random choices and incoming messages made by the adversary. With this new definition of the blinder, Ouafi proved that STRONG-privacy can be ensured. This result is demonstrated with a public-key-based authentication protocol where the encryption scheme is IND-CCA2 secure and PA1+ plaintext-aware. (More details about these security notions can be found in [27].)

5.4.3. Other Extensions. The Vaudenay model has also been broadened in different works. In a nutshell, this is generally performed via the addition of a new oracle to the adversary capabilities (e.g., Timer in [28], MakeInactive in [29], or DestroyReader in [30]) and the corresponding new adversary class (e.g., the TIMEFUL class when $\mathcal{A}$ is allowed to use Timer).

6. Van Le et al. [10, 18], 2007

Also in 2007, van Le et al. introduced a privacy model in [18] (and an extended version in [10]) that is derived from the universal composability (UC) framework [31, 32] (and not on the oracle-based framework). Their aim was to provide security proofs of protocols under concurrent and modular composition, such that protocols can be easily incorporated in more complex systems without reanalyses. Basically, the model, denoted LBM in the following, is based on the indistinguishability between two worlds: the real world and the ideal one.

The transposition of RFID privacy into such a framework is a great contribution since universal composability is considered as one of the most powerful tools for security, especially when composition among several functionalities is required.

6.1. UC Security. General statements about the UC framework are briefly detailed in Appendix A for the reader

nonfamiliar with the field. Here, we present the security notion provided in such a framework.

To prove that an Ident protocol is as secure as the corresponding ideal functionality $\mathcal{F}$, no environment $\mathcal{Z}$ should distinguish if it is interacting with the real adversary $\mathcal{A}$ and Ident (i.e., the real world), or with the simulated adversary *Sim* and $\mathcal{F}$ (i.e., the ideal world). Consequently, $\mathcal{F}$ must be well defined such that all the targeted security properties are trivially ensured. Canetti formally defines this concept in [31] as follows, where PPT denotes probabilistic polynomial time turing machine.

Definition 7 (UC-emulation [31]). A protocol Ident *UC-emulates* a protocol Φ if, for all PPT adversary $\mathcal{A}$, there exists a PPT simulated adversary *Sim* such that, for all PPT environment $\mathcal{Z}$, the distributions $\text{EXEC}_{\text{Ident},\mathcal{A},\mathcal{Z}}$ and $\text{EXEC}_{\Phi,Sim,\mathcal{Z}}$ are indistinguishable.

Based on this security framework, van Le et al. designed in [10, 18] several ideal functionalities to formalize anonymous authentication as well as anonymous authenticated key exchange.

6.2. Description of the LBM Model. The advantage of using this UC-based model is that all the possible adversaries and environments are considered during the security proof that can be carried out with LBM. In this paper, we only focus on the forward-security objective led by anonymous authentication.

6.2.1. Assumptions of an RFID System $\mathcal{S}$. First, the LBM model establishes that the reader $\mathcal{R}$ is the only entity that can start a protocol execution. Then, it considers that only tags can be corrupted by an adversary $\mathcal{A}$. Upon corruption of a tag, $\mathcal{A}$ obtains its keys and all its persistent memory values.

6.2.2. The LBM Ideal Functionality $\mathcal{F}_{aauth}$. This ideal functionality represents the *anonymous authentication* security objective of a given protocol. To do so, several parties (at least $\mathcal{R}$ and one tag) may be involved in a protocol execution. Two parties $\mathcal{P}$ and $\mathcal{P}'$ are said to be *feasible partners* if and only if they are, respectively, $\mathcal{R}$ and a tag. In the ideal world, communication channels between tags and $\mathcal{R}$ are assumed to be anonymous (meaning that they only reveal the type *type*($\mathcal{P}$) of a party, either tag or reader), and a sent message is necessarily delivered to the recipient. Finally, *state*($\mathcal{P}$) is the list of all the execution records, and *active*($\mathcal{P}$) is the list of all the preceding incomplete executions (Box 5).

6.2.3. Forward-*Security.* When the adversary corrupts a tag $\mathcal{T}$, it gets its identifier $\text{ID}_{\mathcal{T}}$ and is then able to impersonate this tag using the IMPERSONATE command. A corrupted tag is thereafter considered as totally controlled by the adversary. Consequently, $\mathcal{F}_{aauth}$ will no longer manage the behavior of this corrupted tag and thus will reject every INITIATE command from this tag. As *state*($\mathcal{T}$) is removed after a corruption, the adversary is not able to link the related tag to its previous authentication.

However, the adversary is able to link all the incomplete protocol executions of a corrupted tag $\mathcal{T}$ up to the last successfully completed one, based on the knowledge of *active*($\mathcal{T}$). Thus, the ideal functionality obviously provides forward-security for all previous completed protocol executions.

7. Van Deursen et al. [13], 2008

The model of van Deursen et al., published in 2008, defines *untraceability* in the standard Dolev-Yao intruder model [33]. The untraceability notion is inspired by the anonymity theory given in [34, 35] and is used as a formal verification of RFID protocols. Such a technique is based on *symbolic protocol analysis* approach (and not on the oracle-based framework). This model will be called DMR in what follows.

7.1. Definition of the System. We remind below the basic definitions given in DMR.

First, the system is composed of a number of *agents* (e.g., Alice or Bob) that execute a *security protocol*, the latter being described by a set of *traces*. A security protocol represents the behavior of a set of *roles* (i.e., initiator, responder, and server), each one specifying a set of actions. These actions depict the role specifications with a sequence of *events* (e.g., sending or reception of a message). A *role term* is a message contained in an event, and it is built from *basic role terms* (e.g., nonces, role names, or keys). A *complex term* is built with functions (e.g., tupling, encryption, hashing, and XOR).

Each trace t is composed of interleaved runs and run prefixes, denoted *subtraces*. A *run* of a role R is a protocol execution from R's point of view, denoted $R\#sid$, where *sid* is a (possibly unique) run identifier. Thus, a run is an instantiation of a role. A *run event* is an instantiation of a role event, that is an instantiation of an event's role terms. A *run term* denotes an instantiated role term. A *run prefix* is an unfinished run.

An adversary $\mathcal{A}$ is in the Dolev-Yao model and is characterized by its *knowledge*. This knowledge is composed of a set of run terms known at the beginning, and the set of run terms that it will observe during its attack. The adversary is allowed to manipulate the information of its knowledge to understand terms or build new ones. However, perfect cryptography is assumed (i.e., cryptographic primitives are assumed unbreakable and considered as black boxes). The inference of term a from term set K is denoted by $K \vdash a$.

Corrupted agents are modeled. (Note that, regarding corruption, there is no restriction about the role of such an agent: it can be either a tag or a reader.) $\mathcal{A}$ is given all the secrets of a corrupted agent in its initial knowledge. When an agent is corrupted, it is said to be "destroyed," that is, it cannot be used during $\mathcal{A}$'s attack. Yet, the security evaluation of a system is done on noncorrupted agents, that is, $\mathcal{A}$ cannot have access to the secret of an agent after the beginning of its attack.

Ideal Functionality $\mathcal{F}_{aauth}$

(i) **Upon receiving** INITIATE **from** $\mathcal{P}$: if $\mathcal{P}$ is corrupted then ignore this message. Else generate a unique execution identification *sid*, record $\texttt{init}(sid, \mathcal{P})$ and send $\texttt{init}(sid, type(\mathcal{P}), active(\mathcal{P}))$ to the adversary.
(ii) **Upon receiving** ACCEPT(sid, sid') **from** the adversary: if there are two records $\texttt{init}(sid, \mathcal{P})$ and $\texttt{init}(sid', \mathcal{P}')$ where $\mathcal{P}$ and $\mathcal{P}'$ are feasible partners, then remove them, record $\texttt{partner}(sid', \mathcal{P}', sid, \mathcal{P})$ and write output **ACCEPT**($\mathcal{P}'$) to $\mathcal{P}$. Else if there is a record $\texttt{partner}(sid, \mathcal{P}, sid', \mathcal{P}')$, then remove it and write output **ACCEPT**($\mathcal{P}'$) to $\mathcal{P}$.
(iii) **Upon receiving** IMPERSONATE($sid, \mathcal{P}'$) **from** the adversary: if there is a record $\texttt{init}(sid, \mathcal{P})$ and party $\mathcal{P}'$ is corrupted, then remove this record and write output **ACCEPT**($\mathcal{P}'$) to $\mathcal{P}$.
(iv) **Upon receiving** CORRUPT(*sid*) **from** the adversary: if there is a record $\texttt{init}(sid, \mathcal{P})$ or $\texttt{partner}(sid, \mathcal{P}, sid', \mathcal{P}')$ such that $\mathcal{P}$ is corruptible, then mark $\mathcal{P}$ as corrupted and remove *state* ($\mathcal{P}$).

Box 5

7.2. Untraceability Notion. First, the model defines several notions of *linkability*, *reinterpretation*, and *indistinguishability*, before giving the *untraceability* one.

Definition 8 (linkability of subtraces [13]). Two subtraces t_i^R and t_j^R are linked, denoted by $L(t_i^R, t_j^R)$, if they are instantiated by the same agent:

$$L\left(t_i^R, t_j^R\right) \equiv \left(\text{agent}\left(t_i^R\right) = \text{agent}\left(t_j^R\right)\right). \tag{6}$$

The notion of *reinterpretation* has been introduced in [34] in order to show that subterms of a message can be replaced by other subterms if the adversary $\mathcal{A}$ is not able to understand these subterms. Note that, when $\mathcal{A}$ is able to understand a subterm, it remains unchanged.

Definition 9 (reinterpretation [13]). A map μ from run terms to run terms is called a reinterpretation under knowledge set K if it and its inverse μ^{-1} satisfy the following conditions:

(i) $\mu(a) = a$ if a is a basic run term,

(ii) $\mu(a) = (\mu(a_1), \ldots, \mu(a_n))$ if $a = (a_1, \ldots, a_n)$ is n-tuple,

(iii) $\mu(\{a\}_{\mathsf{k}}) = \{\mu(a)\}_{\mathsf{k}}$ if $K \vdash \mathsf{k}^{-1}$ or $(K \vdash a \wedge K \vdash \mathsf{k})$, and $\{\cdot\}_{\mathsf{k}}$ is an encryption under key k,

(iv) $\mu(f(a)) = f(\mu(a))$ if $K \vdash a$ or f is not a hash function.

Reinterpretations are used to define *indistinguishability* of traces.

Definition 10 (indistinguishability of traces [13]). Let K be the adversary's knowledge at the end of trace t. The trace t is *indistinguishable* from a trace t', denoted $t \sim t'$, if there is a reinterpretation μ under K, such that $\mu(t_i^R) = t'^R_i$ for all roles R and subtraces t_i^R.

From all the above notions, the untraceability notion of a role is defined as follows.

Definition 11 (untraceability [13]). An Ident protocol is said to be *untraceable* with respect to role R if:

$$(\forall t \in \text{Traces}(\mathsf{Ident}))\ (\forall i \neq j)$$
$$\left(L\left(t_i^R, t_j^R\right) \Longrightarrow \left(\exists t' \in \text{Traces}(\mathsf{Ident})\right)\left(\left(t \sim t'\right) \wedge :L\left(t'^R_i, t'^R_j\right)\right)\right). \tag{7}$$

In this paper, if no role is specified, we consider that "untraceability" means "untraceability for role $\mathcal{T}$."

8. Canard et al. [11, 36], 2010

In the same vein as the Vaudenay model, Canard et al. proposed in 2010 a security model that comprises the properties of (strong) correctness, soundness, and untraceability. We only present the last notion. Contrary to Vaudenay, the authors only defined untraceability (and not privacy in general) and their main goal was to use the strongest adversary of the Vaudenay model. During the following, this model will be denoted CCEG.

8.1. Oracles. As for Vaudenay, DB is empty after the setup of the system, and a tag can be either free or drawn. Then $\mathcal{A}$ has access to all the generic oracles. It may also use the following ones.

(i) DRAWTAG(k) $\rightarrow$ $(\mathcal{T}_1, \ldots, \mathcal{T}_k)$ works similarly as the one of Vaudenay. It first randomly and uniformly selects k tags between all existing (not already drawn) ones. For each chosen tag, the oracle gives it a new pseudonym denoted by $\mathcal{T}_i$ and changes its status from free to drawn. Finally, since $\mathcal{A}$ cannot create here fake tags, then the oracle only outputs all the generated pseudonyms $(\mathcal{T}_1, \ldots, \mathcal{T}_k)$ in any order. If there is not enough free tags (i.e., less than k), then the oracle outputs $\perp$. All relations $(\mathcal{T}_i, \mathsf{ID}_{\mathcal{T}_i})$ are kept in an *a priori* secret table denoted by Tab.

(ii) FREE($\mathcal{T}$) works exactly as the one of Vaudenay.

8.2. Untraceability Experiment. From the oracles given above, CCEG defines three classes of polynomial-time adversaries for the untraceability experiment.

Definition 12 (adversary class [11]). An adversary class is said to be

(i) STRONG if $\mathcal{A}$ has access to all the oracles;

(ii) DESTRUCTIVE if $\mathcal{A}$ cannot use anymore a "corrupted" tag (i.e., the tag has been destroyed);

(iii) WEAK if $\mathcal{A}$ has no access to the CORRUPT oracle;

The authors do not define the NARROW adversary class introduced in the Vaudenay model (see Section 5 for more details). They consider that the model aims to be as powerful as possible: the NARROW notion weakens the adversary.

A *link* is a couple of pseudonyms $(\mathcal{T}_i, \mathcal{T}_j)$ associated to the same identifier in Tab. Some links are considered obvious (e.g., both $\mathcal{T}_i$ and $\mathcal{T}_j$ have been corrupted). Therefore, the authors define the notion of *nonobvious link*. As remark, links are chronologically ordered, that is, $(\mathcal{T}_i, \mathcal{T}_j)$ means that $\mathcal{T}_i$ has been freed before $\mathcal{T}_j$ has been drawn.

Definition 13 (nonobvious link (NOL) [11]). $(\mathcal{T}_i, \mathcal{T}_j)$ is a *nonobvious link* if $\mathcal{T}_i$ and $\mathcal{T}_j$ refer to the same $\mathsf{ID}_{\mathcal{T}}$ in Tab and if a "dummy" adversary $\mathcal{A}_d$, that only has access to CREATETAG, DRAWTAG, FREE, and CORRUPT, is not able to output this link with a probability better than 1/2. Moreover, a nonobvious link is said to be

(i) *standard* if $\mathcal{A}$ has not corrupted $\mathcal{T}_i$ or $\mathcal{T}_j$;

(ii) *past* if $\mathcal{A}$ has corrupted $\mathcal{T}_j$;

(iii) *future* if $\mathcal{A}$ has corrupted $\mathcal{T}_i$.

Note that this model uses a "dummy" adversary $\mathcal{A}_d$, instead of a blinded adversary $\mathcal{A}^{\mathcal{B}}$ as in the Vaudenay model. Both adversaries are equivalent but not identical. Indeed, the main difference is that Vaudenay's blinder $\mathcal{B}$ is an entity clearly separated from $\mathcal{A}^{\mathcal{B}}$. Therefore $\mathcal{B}$ does not know the random choices done by the $\mathcal{A}^{\mathcal{B}}$ during the experiment. On the opposite in CCEG, $\mathcal{A}_d$ is a single entity, and consequently it is aware of its random choices.

A WEAK adversary is only able to output a *standard* NOL as it cannot query the CORRUPT oracle. A DESTRUCTIVE adversary is not able to output a *future* NOL as a tag corruption destroys the tag (and thus prevents the tag from being drawn again). However, this adversary can output a *standard* or *past* NOL. Then, a STRONG adversary is able to output every NOL.

CCEG's untraceability experiment is given in Box 6. P is the adversary class, $P \in \{\mathsf{STRONG}, \mathsf{DESTRUCTIVE}, \mathsf{WEAK}\}$.

8.3. Untraceability Notions. With the previous experiment, the CCEG untraceability of a system $\mathcal{S}$ is proved if no adversary is able to output a NOL with a probability better than the one of the dummy adversary $\mathcal{A}_d$.

Definition 14 (untraceability [11]). An RFID system $\mathcal{S}$ is said to be standard-*untraceable* (resp., past-*untraceable*/future-*untraceable*) if, for every WEAK (resp., DESTRUCTIVE/STRONG) adversary $\mathcal{A}$ running in polynomial-time, it is possible to define a "dummy" adversary $\mathcal{A}_d$ that only has access to oracles CREATETAG, DRAWTAG, FREE, and CORRUPT such that

$$\left|\Pr\left(\mathrm{Exp}^{\mathsf{CCEG\text{-}UNT}}_{\mathcal{S},\mathcal{A}}[\lambda] \text{ succeeds}\right) - \Pr\left(\mathrm{Exp}^{\mathsf{CCEG\text{-}UNT}}_{\mathcal{S},\mathcal{A}_d}[\lambda] \text{ succeeds}\right)\right| \leq \varepsilon(\lambda). \tag{8}$$

Direct implications are made from these notions:

$$\boxed{\text{Future-untraceability} \Longrightarrow \text{Past-untraceability} \Longrightarrow \text{Standard-untraceability}} \tag{9}$$

The main result of this paper is that future-untraceability (the strongest privacy property) is achievable.

9. Deng et al. [12], 2010

Also in 2010, Deng et al. proposed a new framework based on zero-knowledge formulation to define the security and privacy of RFID systems. Here, we only present the *zero-knowledge* privacy (denoted ZK-privacy), which is a new way of thinking in privacy for RFID. This model, denoted DLYZ in the sequel, is part of the *unpredictability models* family [12, 14, 17, 19]. They all rely on the unpredictability of the output returned by a tag or a reader in a protocol execution. In this paper, we decide to only present DLYZ since it is the most achieved model of this family.

9.1. Considered Protocol. This model considers that an RFID protocol execution π is, w.l.o.g., always initialized by $\mathcal{R}$, and π consists of $2\gamma + 1$ rounds for some $\gamma \geq 1$. Each protocol execution π is associated to a unique identifier *sid*. At each execution, a tag may update its internal state and secret key, and $\mathcal{R}$ may update its internal state and database. The update process (of the secret key or the internal state) on a tag always erases the old values. The outputs bits $o^{sid}_{\mathcal{R}}$ and $o^{sid}_{\mathcal{T}}$ (equal to 1 if $\mathcal{R}$ and $\mathcal{T}$ accept the protocol execution with identifier *sid*, or 0 otherwise) are publicly known. Note that the authors claim that each tag $\mathcal{T}$ has its output bit $o^{sid}_{\mathcal{T}} = 0$ if the authentication protocol is not mutual. However, we consider this fact too limiting since $\mathcal{T}$ can have an output (possibly known by $\mathcal{A}$), even if it may not authenticate the reader.

Experiment $\mathrm{Exp}^{\text{CCEG-UNT}}_{\mathcal{S},\mathcal{A}}[\lambda]$

(1) $\mathcal{C}$ initializes the system and sends 1^λ, $\mathcal{S}$'s public parameters param (including K_P) to $\mathcal{A}$.
(2) $\mathcal{A}$ interacts with the whole system, limited by its class P.
(3) $\mathcal{A}$ returns one link $(\mathcal{T}_i, \mathcal{T}_j)$.
$\mathrm{Exp}^{\text{CCEG-UNT}}_{\mathcal{S},\mathcal{A}}$ succeeds if $(\mathcal{T}_i, \mathcal{T}_j)$ is a NOL.

Box 6

For instance, its output can be "I arrived correctly at the end of the protocol on my side."

DLYZ assumes that a tag may participate to at most s executions in its life with $\mathcal{R}$; thus $\mathcal{R}$ is involved in at most sn executions, where s is polynomial in λ and n is the total number of tags involved in the system.

9.2. Oracles. In a nutshell, DLYZ aims to analyze protocols where entities' secrets may potentially be updated at every protocol execution. Therefore, the model automatically enumerates the internal information of each entity. At the initialization of the system, the database is in an initial state, called DB^0, and already stores the secrets of all the tags, that is, a SetupTag has already been performed on every tag. The only differences in the initialization are the following:

(i) SetupReader additionally generates $\mathcal{R}$'s initial internal state $\mathsf{s}^0_{\mathcal{R}}$;

(ii) SetupTag associates to every tag $\mathcal{T}$ a triplet $(\xi_{\mathcal{T}}, \mathsf{k}^0_{\mathcal{T}}, \mathsf{s}^0_{\mathcal{T}})$, which is, respectively, $\mathcal{T}$'s public parameter, initial secret key, and initial internal state.

This information is stored in DB^0. Finally, let $\mathsf{param} = (\mathsf{K_P}, \{\xi_{\mathcal{T}}\}_{\forall \mathcal{T}})$ denote the public parameters of the system $\mathcal{S}$. At the end of the system's initialization, all the tags are accessible to the adversary.

Then, $\mathcal{A}$ has access to the following modified generic oracles.

(i) $\textsc{Launch}() \to (\pi, m)$ makes $\mathcal{R}$ launch a new protocol execution π and generates the 1st-round message m which is also used as the execution identifier *sid*. If this is the jth new execution run by $\mathcal{R}$, then $\mathcal{R}$ stores $\eta_1 = m$ into its internal state $\mathsf{s}^j_{\mathcal{R}}$.

(ii) $\textsc{SendTag}(m, \mathcal{T}) \to r$ sends m to $\mathcal{T}$. The output response r of $\mathcal{T}$ is as follows.

(1) If $\mathcal{T}$ currently does not run any execution, then $\mathcal{T}$
  (a) initiates a new execution with identifier $sid = m$,
  (b) treats m as the 1st-round message of the new execution,
  (c) and returns the 2nd-round message $(sid, r = \alpha_1)$.

(2) If $\mathcal{T}$ is currently running an incomplete execution with identifier *sid* and is waiting for the uth message from $\mathcal{R}$ $(u \geq 2)$, then $\mathcal{T}$ works as follows:
  (a) if $2 \leq u \leq \gamma$, $\mathcal{T}$ treats m as the uth message from $\mathcal{R}$ and returns the next round message $(sid, r = \alpha_u)$;
  (b) if $u = \gamma + 1$ (i.e., the last-round message of the execution), $\mathcal{T}$ returns its output $o^{sid}_{\mathcal{T}}$ and updates its internal state to $\mathsf{s}^{v+1}_{\mathcal{T}}$ (where *sid* corresponds to the vth execution run by $\mathcal{T}$, where $1 \leq v \leq s$).

(iii) $\textsc{SendReader}(m, sid) \to r$ sends m to $\mathcal{R}$ for the execution with identifier *sid*. After receiving m, $\mathcal{R}$ checks from its internal state whether it is running such an execution, and $\mathcal{R}$'s response r is as follows.

(1) If $\mathcal{R}$ is currently running an incomplete execution with identifier *sid* and is waiting for the uth message from a tag $(1 \leq u \leq \gamma)$, then $\mathcal{R}$ works as follows:
  (a) if $u \leq \gamma$, $\mathcal{R}$ treats m as the uth message from the tag and returns the next round message $r = \eta_{u+1}$;
  (b) if $u = \gamma$, $\mathcal{R}$ returns the last-round message $r = \eta_{\gamma+1}$ and its output $o^{sid}_{\mathcal{R}}$ and updates its internal state to $\mathsf{s}^{j+1}_{\mathcal{R}}$ and the database DB^{j+1} (where *sid* corresponds to the jth execution run by $\mathcal{R}$).

(2) In all the other cases, $\mathcal{R}$ returns $\perp$ (for invalid queries).

(iv) $\textsc{Corrupt}(\mathcal{T}) \to (\mathsf{k}^v_{\mathcal{T}}, \mathsf{s}^v_{\mathcal{T}})$ returns the secret key $\mathsf{k}^v_{\mathcal{T}}$ and the internal state $\mathsf{s}^v_{\mathcal{T}}$ currently held by $\mathcal{T}$. Once $\mathcal{T}$ is corrupted, all its actions are controlled and performed by $\mathcal{A}$.

For a completed protocol execution with identifier *sid*, the transcript of the exchanged messages is $(sid, \eta^{sid}_1, \alpha^{sid}_1, \ldots, \alpha^{sid}_\gamma, \eta^{sid}_{\gamma+1})$, excluding the entities' outputs.

Let $\mathcal{O}$ denote the set of these four oracles. $\mathcal{A}^{\mathcal{O}}(\mathcal{R}, T, \mathsf{param})$ denotes a PPT adversary $\mathcal{A}$ that takes on input the system public parameters param, the reader $\mathcal{R}$, and the tags set T of the already initialized system. Then $\mathcal{A}$ interacts with $\mathcal{R}$ and the tags of T via the four oracles. $\mathcal{A}'^{\mathcal{O}}(\mathcal{R}, \widehat{T}, \mathcal{J}(\mathcal{T}_c), \mathsf{aux})$ denotes a PPT adversary $\mathcal{A}'$ equivalent to $\mathcal{A}$, where $\mathsf{aux} \in \{0,1\}^*$ generally includes param

or some historical state information of $\mathcal{A}'$. Then $\mathcal{A}'$ interacts with $\mathcal{R}$ and the tags set $\widehat{T}$ via the four oracles. $\mathcal{A}'$ is said to have a *blinded access* to a *challenge* tag $\mathcal{T}_c \notin \widehat{T}$ if it interacts with $\mathcal{T}_c$ via a special interface $\mathcal{I}$ (i.e., a PPT algorithm which runs $\mathcal{T}_c$ internally and interacts with $\mathcal{A}'$ externally). To send a message m to $\mathcal{T}_c$, $\mathcal{A}'$ sends a SendTag(m, *challenge*) to $\mathcal{I}$; then $\mathcal{I}$ invokes $\mathcal{T}_c$ with SendTag($m, \mathcal{T}_c$) and answers $\mathcal{T}_c$'s output to $\mathcal{A}'$. $\mathcal{A}'$ does not know which tag is interacting with it. $\mathcal{A}'$ interacts with $\mathcal{T}_c$ via SendTag queries only.

Definition 15 (clean tag [12]). A tag $\mathcal{T}$ is said to be *clean* if it is not corrupted (i.e., no query to Corrupt on $\mathcal{T}$) and is not currently running an incomplete execution with $\mathcal{R}$ (i.e., $\mathcal{T}$'s last execution is either finished or aborted).

The main goal of this definition is to force the adversary to use some uncorrupted and nonrunning tags to proceed the ZK-privacy experiment (see next section). This notion of nonrunning tags is very similar to the TagInit oracle of JW.

9.3. Privacy Experiments. In the experiments, a PPT CMIM (concurrent man-in-the-middle) adversary $\mathcal{A}$ (resp., PPT simulator *Sim*) is composed of a pair of adversaries $(\mathcal{A}_1, \mathcal{A}_2)$ (resp., (Sim_1, Sim_2)) and runs in two stages. Note that, if $\delta = 0$, then no challenge tag is selected, and $\mathcal{A}$ is reduced to $\mathcal{A}_1$ in the experiment.

The first experiment given in Box 7 is the one performed by the real adversary $\mathcal{A}$. After the system initialization, $\mathcal{A}_1$ plays with all the entities and returns a set of clean tags C. Then from this set C, a challenge tag $\mathcal{T}_c$ is chosen at random. Then $\mathcal{A}_2$ plays with all the entities, including the challenge tag via the interface $\mathcal{I}$, except the set of clean tags. At the end, $\mathcal{A}$ outputs a view of the system.

Then, the second experiment given in Box 8 is the one performed by the simulator *Sim*. As in the previous experiment, Sim_1 plays with all the entities and returns a set of clean tags C. Then from this set C, a challenge tag $\mathcal{T}_c$ is chosen at random, but *Sim* is not informed about its identity and cannot play anymore with this tag. Then Sim_2 plays with all the entities, except the set of clean tags. At the end, *Sim* outputs a simulated view of the system.

9.4. Privacy Notions. From the previous experiments, the ZK-privacy of a system $\mathcal{S}$ is proved when no one is able to distinguish if it is interacting with the real world or with the simulated one.

Definition 16 (ZK-privacy [12]). An RFID system $\mathcal{S}$ satisfies computational (resp., statistical) ZK-*privacy* if, for any PPT CMIM adversary $\mathcal{A}$, there exists a polynomial-time simulator *Sim* such that, for all sufficiently large λ and any n which is polynomial in λ, the following ensembles are computationally (resp., statistically) indistinguishable:

(i) $\{c, view_{\mathcal{A}}(\lambda, n)\}_{\lambda \in \mathbb{N}, n \in \text{poly}(\lambda)}$,

(ii) $\{c, sview(\lambda, n)\}_{\lambda \in \mathbb{N}, n \in \text{poly}(\lambda)}$.

That is, for any polynomial-time (resp., any computationally power unlimited) algorithm $\mathcal{D}$, it holds that

$$\left|\Pr[\mathcal{D}(\lambda, n, c, view_{\mathcal{A}}(\lambda, n)) = 1] - \Pr[\mathcal{D}(\lambda, n, c, sview(\lambda, n)) = 1]\right| = \varepsilon(\lambda). \quad (10)$$

The probability is taken over the random coins used during the system initialization, the random coins used by $\mathcal{A}$, *Sim*, $\mathcal{R}$, and all (uncorrupted) tags, the choice of c, and the coins used by the distinguisher algorithm $\mathcal{D}$.

Definition 17 (Forward/Backward-ZK-privacy [12]). Let us denote $(\mathsf{k}^{\text{final}}_{\mathcal{T}_c}, \mathsf{s}^{\text{final}}_{\mathcal{T}_c})$ (resp., $(\mathsf{k}^{0}_{\mathcal{T}_c}, \mathsf{s}^{0}_{\mathcal{T}_c})$) the final (resp., initial) secret key and internal state of the challenge tag $\mathcal{T}_c$ at the end (resp., beginning) of $\text{Exp}^{\text{ZK-priv}}_{\mathcal{S},\mathcal{A}}$. An RFID system $\mathcal{S}$ is forward (resp., backward)-ZK-*private* if, for any PPT CMIM adversary $\mathcal{A}$, there exists a polynomial-time simulator *Sim* such that, for all sufficiently large λ and any n which is polynomial in λ, the following distributions are indistinguishable:

(i) $\{\mathsf{k}^{\text{final}}_{\mathcal{T}_c}, \mathsf{s}^{\text{final}}_{\mathcal{T}_c}(\text{resp.}, \mathsf{k}^{0}_{\mathcal{T}_c}, \mathsf{s}^{0}_{\mathcal{T}_c}), c, view_{\mathcal{A}}(\lambda, n)\}$,

(ii) $\{\mathsf{k}^{\text{final}}_{\mathcal{T}_c}, \mathsf{s}^{\text{final}}_{\mathcal{T}_c}(\text{resp.}, \mathsf{k}^{0}_{\mathcal{T}_c}, \mathsf{s}^{0}_{\mathcal{T}_c}), c, sview(\lambda, n)\}$.

It is required that $\mathcal{T}_c$ should remain clean at the end of $\text{Exp}^{\text{ZK-priv}}_{\mathcal{S},\mathcal{A}}$. Note that $\mathcal{A}$ is allowed to corrupt it after the end of $\text{Exp}^{\text{ZK-priv}}_{\mathcal{S},\mathcal{A}}$.

One justification of the authors on the way of corrupting $\mathcal{T}_c$ is that it is enough to give its secrets to $\mathcal{A}$ at the end. Another reason pointed out by the authors is that forward-ZK or backward-ZK-privacy cannot be achieved if $\mathcal{A}$ corrupts $\mathcal{T}_c$ before the end of the experiment.

10. Hermans et al. [15], 2011

Following the path opened by Vaudenay with his privacy model, Hermans et al. presented in 2011 a new model, denoted here HPVP, based on indistinguishability between two "worlds": it is most commonly called the "left-or-right" paradigm.

The main goal of the authors was to propose a model with a clear defined purpose, that is straightforward to use for proving privacy. Also as CCEG, HPVP aimed to use Vaudenay's strongest adversary.

10.1. Oracles. As for Vaudenay and CCEG, DB is empty after the initialization of the system, and a tag can be either free or drawn. Then $\mathcal{A}$ has access to the generic oracles CreateTag (here it additionally returns a reference $\mathcal{T}$ to the new created tag), SendReader, and Result. Then, $\mathcal{A}$ has also access to these other following oracles.

(i) DrawTag($\mathcal{T}_i, \mathcal{T}_j$) $\rightarrow$ $\mathcal{T}_{\text{drawn}}$ generates a drawn tag $\mathcal{T}_{\text{drawn}}$ and stores $(\mathcal{T}_{\text{drawn}}, \mathcal{T}_i, \mathcal{T}_j)$ in a table Tab. Depending on the bit b chosen at the start of the privacy experiment (see next section), $\mathcal{T}_{\text{drawn}}$ will either reference $\mathcal{T}_i$ or $\mathcal{T}_j$. If one of the two tags $(\mathcal{T}_i, \mathcal{T}_j)$ is already referenced in Tab, then it outputs $\perp$.

Experiment $\mathrm{Exp}^{\mathsf{ZK\text{-}priv}}_{\mathcal{S},\mathcal{A}}[\lambda, n]$ (real world)

(1) $\mathscr{C}$ initializes the system and sends 1^λ, param to $\mathscr{A}$.
(2) $\{C,\mathsf{info}\} \leftarrow \mathscr{A}_1^{\mathcal{O}}(\mathcal{R}, T,\mathsf{param})$, where $C = \{\mathcal{T}_{i_1}, \mathcal{T}_{i_2}, \ldots, \mathcal{T}_{i_\delta}\} \subseteq T$ is a set of *clean* tags $(0 \le \delta \le n)$, and info is a state information.
(3) $c \in_R \{1, \ldots, \delta\}$, set $\mathcal{T}_c = \mathcal{T}_{i_c}$ and $\widehat{T} = T - C$.
(4) $view_{\mathscr{A}} \leftarrow \mathscr{A}_2^{\mathcal{O}}(\mathcal{R}, \widehat{T}, \mathcal{I}(\mathcal{T}_c),\mathsf{info})$.
(5) Output $(c, view_{\mathscr{A}}(\lambda, n))$.

Box 7

Experiment $\mathrm{Exp}^{\mathsf{ZK\text{-}priv}}_{\mathcal{S},Sim}[\lambda, n]$ (simulated world)

(1) $\mathscr{C}$ initializes the system and sends 1^λ, param to $\mathscr{A}$.
(2) $\{C,\ \mathsf{info}\} \leftarrow Sim_1^{\mathcal{O}}(\mathcal{R}, T,\mathsf{param})$, where $C = \{\mathcal{T}_{i_1}, \mathcal{T}_{i_2}, \ldots, \mathcal{T}_{i_\delta}\} \subseteq T$ is a set of *clean* tags $(0 \le \delta \le n)$, and info is a state information.
(3) $c \in_R \{1, \ldots, \delta\}$ unknown to *Sim*, and set $\widehat{T} = T - C$.
(4) $sview \leftarrow Sim_2^{\mathcal{O}}(\mathcal{R}, \widehat{T},\ \mathsf{info})$, where *sview* includes all oracle answers to queries made by *Sim*.
(5) Output $(c, sview(\lambda, n))$.

Box 8

(ii) $\textsc{Free}_b(\mathcal{T}_{\mathsf{drawn}})$ recovers the tuple $(\mathcal{T}_{\mathsf{drawn}}, \mathcal{T}_i, \mathcal{T}_j)$ in Tab. If $b = 0$ then it resets $\mathcal{T}_i$, otherwise it resets $\mathcal{T}_j$. Then it removes the tuple from Tab. When a tag is reset, its volatile memory is erased, not its nonvolatile memory (which contains its secret $\mathsf{k}_{\mathcal{T}}$).

This specific definition of the Free oracle comes from one important statement highlighted by Paise and Vaudenay in their model (see Section 5.4 for more details).

Finally $\mathscr{A}$ has access to the following modified generic oracles.

(i) $\textsc{Launch}() \rightarrow (\pi, m)$ makes $\mathcal{R}$ launch a new Ident protocol execution π, together with $\mathcal{R}$'s first message m.

(ii) $\textsc{SendTag}(m, \mathcal{T}) \rightarrow r$ retrieves the tuple $(\mathcal{T}, \mathcal{T}_i, \mathcal{T}_j)$ in Tab. It sends a message m to the corresponding tag ($\mathcal{T}_i$ if $b = 0$, $\mathcal{T}_j$ otherwise). It outputs the response r of the tag. If $\mathcal{T}$ is not found in Tab, it returns $\perp$.

(iii) $\textsc{Corrupt}(\mathcal{T}) \rightarrow \mathsf{k}_{\mathcal{T}}$ returns the whole memory (including the current secret $\mathsf{k}_{\mathcal{T}}$) of $\mathcal{T}$. If $\mathcal{T}$ is drawn, it returns $\perp$.

All these oracles are very similar to the ones of Vaudenay, but with important differences. First, DrawTag is only applied on two tags chosen by the adversary when it queries this oracle. Then, Free specifies clearly that it erases the volatile memory of the chosen tag. Lastly, Corrupt is only authorized on a free tag. However, the intrinsic definition of a free tag (given in the Vaudenay model [22]) is that it is not accessible to $\mathscr{A}$, since it is not in its neighborhood. Thus, it seems impossible for $\mathscr{A}$ to query a Corrupt on a tag that it cannot manipulate (i.e., not drawn).

10.2. Privacy Experiment. The authors keep the same adversary classes as the ones given by Vaudenay: STRONG, DESTRUCTIVE, FORWARD, WEAK, and NARROW.

Their privacy experiment is given in Box 9, where P represents the adversary class: $P \in \{\varnothing, \mathsf{NARROW}\} \times \{\mathsf{WEAK}, \mathsf{FORWARD}, \mathsf{DESTRUCTIVE}, \mathsf{STRONG}\}$.

10.3. Privacy Notions. From the previous experiment, the HPVP privacy property is based on the adversary advantage to distinguish the two worlds.

Definition 18 (privacy [15]). The RFID system $\mathcal{S}$ is said to unconditionally (resp., computationally) provide *P-privacy* if and only if, for all the adversaries (resp., polynomial time adversaries) which belong to class P, it holds that

$$\begin{aligned}&\left|\Pr\left(\mathrm{Exp}^{\mathsf{HPVP\text{-}Priv}}_{\mathcal{S},\mathcal{A}}[\lambda, 0]\ \text{ succeeds}\right)\right.\\&\qquad\left.+\Pr\left(\mathrm{Exp}^{\mathsf{HPVP\text{-}Priv}}_{\mathcal{S},\mathcal{A}}[\lambda, 1]\ \text{ succeeds}\right) - 1\right| \qquad (11)\\&= 0 \quad (\text{resp.} \le \varepsilon(\lambda)).\end{aligned}$$

Note that, all along the paper, the authors claim that the already existing models do not take care about some privacy leakage information such as the cardinality of the tags' set. Yet, they never prove nor explain how their model can handle this issue, nor why this is indeed a privacy issue.

11. Privacy Analysis of Different Existing Protocols

To investigate more deeply the differences between the presented models, we study the privacy level of five different protocols in all these models. These protocols differ

Experiment $\mathrm{Exp}^{\mathsf{HPVP\text{-}priv}}_{\mathcal{S},\mathcal{A}}[\lambda, b]$

(1) $\mathcal{C}$ initializes the system, chooses a random bit b, and sends 1^λ and $\mathcal{S}$'s public parameters param to $\mathcal{A}$.
(2) $\mathcal{A}$ interacts with the whole system, limited by its class $\mathcal{P}$.
(3) $\mathcal{A}$ outputs a guess bit b'.
$\mathrm{Exp}^{\mathsf{HPVP\text{-}priv}}_{\mathcal{S},\mathcal{A}}$ succeeds if $b = b'$.

Box 9

according to their building blocks and their underlying key infrastructure. The first protocol [37] is based on unique long-term secret key for each tag. On the contrary in the tree-based protocol [8], tags share between them some long-term partial secret keys so as to speed up the authentication. Two protocols [18, 38] use key-update mechanisms to increase the privacy level in case of tag corruption. In particular, the second one [18] provides mutual authentication in order to be undesynchronizable. The last analyzed protocol [22] is based on public-key cryptography. Due to their differences, these protocols may thus ensure different privacy levels. However, we will show in this section that some models assign the same privacy level to some protocols while other models clearly differentiate them, for example, by taking into account an attack which cannot be modeled in other models.

In the following, a tag $\mathcal{T}$ has a unique identifier $\mathsf{ID}_\mathcal{T}$ and should be authenticated by a legitimate reader $\mathcal{R}$.

11.1. Analyzed Protocols. The five RFID protocols chosen for this study are sketched in the following. Their complete descriptions and whole privacy analyses are detailed in Appendix B.

11.1.1. SK-Based Challenge/Response Authentication Protocol. The first studied protocol is the ISO/IEC 9798-2 Mechanism 2 [37] based on a PRF with an additional nonce chosen by the tag. A tag $\mathcal{T}$ has a unique secret key $\mathsf{k}_\mathcal{T}$ known by $\mathcal{R}$, used for the authentication. All the tags' keys are independent.

11.1.2. Tree-Based Authentication Protocol. It is based on the key-tree infrastructure given by Molnar and Wagner in [8]. Basically in a system of n tags, a key-tree is generated with $\beta^d \geq n$ leaves, where d is its depth and β is its branching factor. Each leaf is randomly associated to a tag $\mathcal{T}$ of the system, and each node is associated to a partial unique secret key $\mathsf{k}_{i,j}$ where i is the depth of the node and j the branch.

We define w.l.o.g. $(p_0, p_1, p_2, \ldots, p_d)$ the path in the tree from the root (denoted p_0) to the leaf (denoted p_d) that is associated to the tag $\mathcal{T}$. At the setup of the system, $\mathcal{T}$ is initialized with a set of partial keys $\{\mathsf{k}_{p_1}, \mathsf{k}_{p_2}, \ldots, \mathsf{k}_{p_d}\}$, where each k_{p_i} is the secret key attached to its path node p_i (except the root). $\mathcal{R}$ knows the entire tree arrangement, and thus all the keys associated to all the nodes.

The protocol is carried out in d rounds. For each round, $\mathcal{R}$ and $\mathcal{T}$ perform a challenge/response authentication as described in Figure 2 of Appendix B.2. If $\mathcal{T}$ answers correctly at each round, then $\mathcal{R}$ successfully authenticates $\mathcal{T}$ at the end of the last round.

11.1.3. OSK-Based Authentication Protocol. The original OSK protocol [38] is an identification protocol, where there is no proof of the tag identity. At the setup, $\mathcal{T}$ is initialized with a unique secret key $\mathsf{k}_\mathcal{T}$ shared with $\mathcal{R}$. All the tags' keys are independent. $\mathcal{T}$ just sends the result of a pseudorandom function done on its key. The main feature of OSK is that $\mathcal{T}$ and $\mathcal{R}$ update the shared key after each complete protocol execution.

The OSK protocol has been introduced to ensure the *forward security* property, that is, data sent by a given tag $\mathcal{T}$ today will still be secure even if $\mathcal{T}$'s secret is disclosed by tampering this tag in the future, contrary to the SK-based protocol. The protocol presented here (proposed in [22]) is slightly different from OSK as $\mathcal{R}$ additionally sends a nonce to $\mathcal{T}$ in order to prevent replay attacks, as described in [6]. The resulting protocol ensures tag authentication rather than tag identification.

11.1.4. O-FRAP Authentication Protocol. Many undesynchronizable authentication protocols [18, 24, 39] have been proposed to counter the main drawback of OSK, that is the desynchronization attack. Here, we analyze O-FRAP, introduced by van Le et al. in [18].

At the setup, $\mathcal{T}$ is initialized with a couple containing a secret key and a nonce $(\mathsf{k}_\mathcal{T}, n_\mathcal{T})$, such that all the couples of tags are independent. $(\mathsf{k}_\mathcal{T}, n_\mathcal{T})$ is stored by $\mathcal{R}$ as the current secrets $cur_\mathcal{T}$ of $\mathcal{T}$. Then a mutual authentication between $\mathcal{R}$ and $\mathcal{T}$ is performed, where $\mathcal{T}$'s key and/or nonce are updated at the end of the protocol execution by both entities. The main difference with OSK is that the tag always updates at least one value, even when the protocol is incomplete (in this case the random $n_\mathcal{T}$).

11.1.5. PK-Based Challenge/Response Authentication Protocol. It is one of the protocols given by Vaudenay in [22]. $\mathcal{R}$ has a pair of public/private keys $(\mathsf{K_P}, \mathsf{K_S})$, and a tag $\mathcal{T}$ has a unique secret key $\mathsf{k}_\mathcal{T}$ known by $\mathcal{R}$. All the tags' keys are independent. The encryption scheme (Enc/Dec) is considered to be either IND-CPA (indistinguishable under chosen-plaintext attack) or IND-CCA (indistinguishable under chosen-ciphertext attack) secure.

11.2. Analysis Comparison. Table 1 sums up the security analysis of the studied protocols regarding each privacy model.

11.2.1. The Lack of Comprehensiveness. In some models, several protocols are proved to ensure the same privacy level, because some attacks on these protocols cannot be formalized. For example in the Avoine model, OSK-based, O-FRAP, and PK-based protocols reach the same privacy (i.e., Existential-UNT-RTE and Forward-UNT-RTEC). However as detailed in Appendix B.3, the OSK-based protocol can be desynchronized contrary to the other two, and O-FRAP is subject to a specific attack based on tag corruption (see Appendix B.4), while the PK-based protocol is not vulnerable to such attacks. This misevaluation of privacy happens in almost all models (e.g., {SK-based, tree-based, O-FRAP} for Vaudenay, CCEG, and HPVP, or {SK-based, OSK-based, O-FRAP} for DMR). The main drawback of this fact is that system designers unfamiliar with privacy will probably choose the cheapest protocol (regarding the computing complexity), thinking that these protocols are equivalent regarding their privacy level.

11.2.2. The Case of Correlated Secrets. Nevertheless, some models have features that permit attributing different privacy levels to quite similar protocols. As an example, JW, DMR, and DLYZ point out an important characteristic of protocols based on correlated secrets: they prove that the tree-based protocol is not secure, while the SK-based one is. This comes from the fact that an adversary may know some secrets without being authorized to corrupt the challenge tags (as explained in Appendix B.2). For instance, this adversary could be a tag owner that only knows its tags' secrets and that is not able to corrupt other tags that it wants to trace. It is consequently normal that the SK-based protocol is more private than the tree-based one. Note that this differentiation cannot be established in the Avoine, Vaudenay, CCEG, and HPVP models because their adversary does not have the modularity to only corrupt certain tags. As a consequence, these models classify the SK-based and the tree-based protocols with the same privacy level.

11.2.3. The Key-Update Mechanism Dilemma. All the models (except Avoine and LBM) give the same privacy level for the SK-based protocol and for O-FRAP. This is another obvious example about the issue related to the privacy definitions of these models. Indeed, the two protocols do not manage the tags' secrets in the same way: a tag updates one of its secrets each time it starts an execution of O-FRAP, while a tag always keeps the same secret when it runs the SK-based protocol. For O-FRAP, the attack presented in Appendix B.4 only permits linking a freshly corrupted tag to its last previous incomplete protocol execution. But all the previous completed ones are unlinkable. This is not the case with the SK-based protocol, where a tag corruption allows tracing the tag at any time (past or future). This obvious distinction of the two protocols is however not highlighted by most of the models.

11.2.4. Accuracy Refinement of the NARROW *Adversary.* The NARROW nuance provided in some models permits granting some protocols with a reasonable privacy level. For instance, Vaudenay and HPVP confer NARROW-DESTRUCTIVE-privacy on the OSK-based protocol and NARROW-STRONG-privacy on the IND-CPA-PK-based protocol, while some other models argue that the OSK-based protocol ensures no privacy at all or that the IND-CPA-PK-based protocol cannot be proved private. These last claims are highly restrictive since these two protocols are clearly more private than the dummy identification protocol where tags send their identifier in the clear.

11.2.5. The Vaudenay Problem. Finally, Vaudenay proved in [22] that the highest privacy level of his model cannot be achieved. Yet, the highest privacy level of all the other seven presented models can be reached, at least with the IND-CCA-PK-based protocol. To the best of our knowledge, Ouafi is the only author who tries to explain in [20] that the Vaudenay model (i) does not reflect the exact notion of privacy that was targeted at first sight and (ii) may englobe more than only privacy. As explained in Section 5.4, Ouafi reformulates the Vaudenay model in order to achieve STRONG-privacy.

12. Classification of the Models

In this section, we compare the different features of all the privacy models presented in this paper. We point out which model(s) is(are) the most appropriate to use according to whether one of these features is wished or not. Table 2 sums up the features that are achieved by each model.

Note that "protocols" (resp., "tag-init protocols") refer to authentication/identification protocols where the reader (resp., tag) is the only entity that can start a protocol execution.

12.1. Adversary Experiment. Privacy models can be compared according to the similarities and differences of their experiment. To do so, we first need to define the notion of *challenge tags* in some models. Indeed, Vaudenay, LBM, DMR, CCEG, and HPVP do not stipulate this specific notion in their experiment. However, since their adversary must use some tags for its attack, we consider that all the tags are challenge ones. Note that the agents that can be corrupted before $\mathcal{A}$'s attack in the DMR model are considered as *nonchallenge tags*.

12.1.1. Number of Tags Allowed in the Experiment. Vaudenay, LBM, and CCEG are the only models where the adversary $\mathcal{A}$ is free to play with all the tags of the system at the same time during its attack.

At one moment of their experiment, JW and HPVP can only play with at most $(n - 1)$ tags (where n is the total number of tags of the studied system). For the DLYZ model, the adversary cannot play with the set of clean tags it chose, except with the challenge tag $\mathcal{T}_c$ picked at random in this set. If this set contains only two tags, it can however play with at most $(n - 1)$ tags. Then, DMR's adversary cannot play with the agents that were corrupted before the beginning of its attack. Finally, the Avoine model is the most limiting one, since $\mathcal{A}$ can only play with two tags. This fact prevents

Table 1: Analysis summary of the protocols. "✗" means no privacy. For the PK-based protocol, a property followed by "*" means that it is at least achieved with IND-CPA-security. For the sake of clarity, we denote "N" and "DESTR" as being, respectively, "NARROW" and "DESTRUCTIVE."

Model	Protocol				
	SK based [37]	Tree based [8]	OSK based [22]	O FRAP [18]	PK based [22]
Avoine	Existential-UNT-RTE	Existential-UNT-RTE	Existential-UNT-RTE Forward-UNT-RTEC	Existential-UNT-RTE Forward-UNT-RTEC	Existential-UNT-RTE* Forward-UNT-RTEC*
JW	(ρ, σ, τ)-privacy	✗	✗	(ρ, σ, τ)-privacy	Forward-(ρ, σ, τ)-privacy
Vaudenay	WEAK-privacy	WEAK-privacy	N-DESTR-privacy	WEAK-privacy	N-STRONG-privacy* FORWAD-privacy
LBM	✗	✗	✗	Forward-security	Forward-security
DMR	Untraceability	✗	Untraceability	Untraceability	Untraceability*
CCEG	Standard-untraceability	Standard-untraceability	✗	Standard-untraceability	Future-untraceability
DLYZ	ZK-privacy	✗	✗	ZK-privacy	Backward-ZK-privacy
HPVP	WEAK-privacy	WEAK-privacy	N-DESTR-privacy	WEAK-privacy	N-STRONG-privacy* STRONG-privacy

Table 2: Comparison of the presented privacy models. "✓" (resp., "✗") means that the feature is (resp., is not) given to the adversary $\mathcal{A}$. "N/A" means that the feature is not applicable in the model.

Feature	Model							
	Avoine	JW	Vaudenay	LBM	DMR	CCEG	DLYZ	HPVP
Interaction with all the tags	Only 2 tags	not $\mathcal{T}^*_{b\oplus 1}$	✓	✓	not corrupted agents	✓	not all clean tags	all-but-one
Choice of the challenge tags	✗	✓	✓	✓	✓	✓	✓	✓
Attack on incomplete executions	Both	✓	✓	✗	✓	✓	✓	✓
Corrupt challenge tags	Only $\mathcal{T}$	Only $\mathcal{T}^*_b$	✓	✓	✗	✓	✗	✓
Corrupt nonchallenge tags	N/A	✓	N/A	N/A	✓	N/A	✓	N/A
Corrupt any tag	✗	✗	✓	✓	✗	✓	✗	✓
NARROW/WIDE	NARROW	WIDE	both	WIDE	NARROW	WIDE	WIDE	Both
Channels asymmetry	✓	✗	✗	✗	✗	✗	✗	✗
Protocols analyzable	3-pass with independent secrets	SK based	all	all	all	all	$(2\gamma + 1)$-pass	All
Tag-init protocols analyzable	✗	✓	✗	✗	✓	✗	✗	✗

the Avoine model from analyzing protocols with correlated secrets, which is not the case for all the other models.

Therefore, if $\mathcal{A}$ is allowed to play with all the tags of the system, then it is preferable to use the Vaudenay, LBM, and CCEG models for the privacy analysis.

12.1.2. Choice of the Challenge Tags. All the models (except the Avoine one) allow $\mathcal{A}$ to choose the challenge tags of its attack. In the Avoine model, the challenger $\mathcal{C}$ is the entity that performs this task, choosing $\mathcal{T}$, $\mathcal{T}_0$, and $\mathcal{T}_1$ (such that $\mathcal{T} = \mathcal{T}_0$ or $\mathcal{T}_1$). $\mathcal{A}$ has no option on the tags used for its attack: it is weaker than the adversaries of the other models. Thus, if it is considered that $\mathcal{A}$ has the possibility to choose the challenge tags, protocol should be analyzed with all the models except the Avoine one.

12.1.3. Attack on Incomplete Protocol Executions. In the JW, Vaudenay, DMR, CCEG, DLYZ, and HPVP models, $\mathcal{A}$ is allowed to perform its attack on incomplete protocol executions. As illustrated in Appendix B.4, it can start an execution with a tag and not finish it. Afterward, it can use this tag during its game to break its privacy. If $\mathcal{A}$ succeeds to do so, then the protocol is not considered as private.

For LBM, such an attack is not taken into account. $\mathcal{F}_{aauth}$ is designed such that all the successfully completed protocol executions of a tag are protected against corruption. In other words, $\mathcal{A}$ cannot learn any information about these previous executions, and thus the privacy of a tag is ensured. However, it is authorized to link the previous incomplete executions of a corrupted tag up to the last completed one without compromising the security.

For the Avoine model, both scenarios are allowed. During the Existential game, $\mathcal{A}$ chooses the intervals I_0 and I_1 of the challenge tags that help it the most to perform its attack. It can choose I_0 and I_1 such that these intervals are directly consecutive to I (the interval of the targeted tag $\mathcal{T}$). In that case, nothing prevents $\mathcal{A}$ from using incomplete protocol executions during the experiment. For the Universal game, the challenger $\mathcal{C}$ is the one that chooses I_0 and I_1 that

help $\mathscr{A}$ the less, contrary to the Existential game. If $\mathscr{A}$ uses incomplete protocol executions, then $\mathscr{C}$ can choose nonconsecutive intervals such that the incomplete executions remain meaningless to $\mathscr{A}$ (as for LBM). For instance, some completed executions may separate the executions (completed or not) performed within the intervals.

Therefore, if a protocol must be protected against this attack, then Avoine, JW, Vaudenay, DMR, CCEG, DLYZ, and HPVP are the most appropriate models to study its privacy. If such a feature is not wished, then it can be analyzed with the Avoine and LBM models. Note that the Avoine model is the most flexible one since it can handle both scenarios.

12.2. Tag Corruption. The tamper resistance of RFID tags is a highly questionable assumption. Fortunately, all the models are flexible regarding the capacity of an adversary to corrupt tags. The two extreme cases are the impossibility to corrupt tags or the possibility to perform this action without restrictions. Yet, as detailed in the previous sections, intermediate levels of corruption have been introduced. To have an overall view of these levels, the models are gathered below based on their similarities from the weakest corruption level to the strongest one.

12.2.1. Weak Adversary. Obviously the weakest corruption level is when $\mathscr{A}$ is not allowed to corrupt tags. This feature is present in the Avoine, Vaudenay, LBM, CCEG and HPVP models. It permits formalizing the assumption of tags tamper resistance.

Although the JW, DMR and DLYZ models consider that it is always possible to corrupt non-challenge tags, they also define a weak level of corruption where $\mathscr{A}$ is not able to corrupt the challenge tags. This adversary, called *insider adversary* in [40], may be a tag owner that only knows its tags' secrets and that wants to break the privacy of other tags. As explained in Section 11.2 and in Appendix B.2, this subtle adversary can be used to perform a dedicated attack on a system with correlated secrets. However, even if this attack can be caught in other models by an overpowerful adversary (e.g., Vaudenay's FORWARD adversary), the Vaudenay, LBM, CCEG, and HPVP models are unable to precisely formalize such an intermediate adversary, since these models allow $\mathscr{A}$ to corrupt either every tag or any tag at all.

Therefore on the one hand, if it is assumed that $\mathscr{A}$ can never corrupt a tag, then the Avoine, Vaudenay, LBM, CCEG, and HPVP models should be chosen for a protocol analysis. On the other hand, if it is assumed that only the nonchallenge tags can be corrupted, then the most appropriate and fair models to use are JW, DMR, and DLYZ.

12.2.2. Nonadaptive Adversary. A higher level of corruption consists in authorizing $\mathscr{A}$ to only corrupt tags at the end of the experiment. It corresponds to the FORWARD adversary of Vaudenay and HPVP and to the Forward-UNT notion of Avoine. It can be viewed as a nonadaptive corruption ability as, except other corruptions, $\mathscr{A}$ cannot adapt its attack according to the corruption result.

The forward-ZK-privacy of DLYZ is close to this property since the last key of the challenge tag is given to the distinguisher at the end of the experiment. Yet in this case, $\mathscr{A}$ is still allowed to adaptively corrupt the nonchallenge tags during the experiment without stopping it. This fact slightly increases the strength of DLYZ's adversary.

12.2.3. Destructive Adversary. To increase the adversary power, some models give $\mathscr{A}$ the ability to pursue its attack after a corruption, leading to adaptive attacks regarding corruption. However, some constraints are still put into place in some models. In fact, the JW model considers that the challenge tags may be corrupted in the forward-(ρ, σ, τ)-privacy, but only during the challenge phase. In other words, a tag corruption can only be used to trace its previous interactions. It is thus possible to establish a parallel between this constraint and the destructive corruption ability defined in other models (i.e., the DESTRUCTIVE adversary of Vaudenay, CCEG and HPVP, and the forward-security of LBM). Indeed, the key material obtained through a tag corruption may allow tracing its previous interactions but not the future ones as the tag is destroyed.

12.2.4. Strong Adversary. The strongest level that can be defined is obviously when $\mathscr{A}$ has no restriction regarding tag corruption. This corresponds to the STRONG adversary defined in the Vaudenay, CCEG, and HPVP models. A relatively similar notion is also defined by DLYZ, namely, the backward-ZK-privacy. However, as for the forward-ZK-privacy, while every nonchallenge tag may be corrupted during the experiment, the challenge tag cannot, and its initial key is only revealed at the end of the experiment. It may still help to distinguish the following interactions of this tag, but $\mathscr{A}$ cannot adapt its attack to this result. This consequently leads to a nonadaptive adversary that may be useful in some cases. Nevertheless, one may prefer the Vaudenay, CCEG, and HPVP models to catch the strongest adversary definition regarding corruption ability.

As a conclusion, the Vaudenay, CCEG, and HPVP models offer a wider adversary granularity regarding tag corruption. (Note that the CCEG's authors consider that FORWARD and DESTRUCTIVE adversaries (in Vaudenay's sense) are equivalent in their experiment: both are able to output a *standard* or *past* NOL, but not a *future* NOL. Therefore, a FORWARD adversary is useless in their model.) Only these three models take into account the strongest adversary which can corrupt with no restriction. Nevertheless, they do not consider the insider adversary that represents a relevant assumption and affords, to our mind, an interesting granularity for some analyses. In this case, protocols may thus be studied with a more appropriate model, namely, either JW, or DMR, or DLYZ.

12.3. Other Features. The remaining features of Table 2 are discussed in the following.

12.3.1. NARROW/WIDE *Adversaries.* As previously said, an adversary $\mathscr{A}$ is said to be NARROW (resp., WIDE) when

it does not (resp., does) receive the result of a protocol execution. Several models restrict their adversary with one of these features.

Avoine does not define a Result oracle, and there is no equivalence of such an oracle in DMR (since $\mathscr{A}$ does not know if a protocol between two agents succeeds). Both models only consider NARROW adversaries.

On the contrary, the adversaries of JW, LBM, CCEG, and DLYZ are only WIDE ones. For JW, there is no Result oracle defined in the model, but the adversary is forced to obtain the result of a protocol execution via the output of each SendReader. The DLYZ's adversary has the same behavior: it is forced to know this result information since $o_{\mathscr{R}}^{sid}$ and $o_{\mathscr{T}}^{sid}$ are public. In the LBM model, the output tape of each party is always available to $\mathscr{Z}$. Additionally, the adversary may also learn it as $\mathscr{Z}$ can communicate arbitrarily with it. Thus, it is impossible to model a NARROW adversary since the distinguisher may always know the result of a protocol execution. For CCEG, no NARROW adversary can be used for the untraceability experiment. Yet, as stressed in OSK's analysis given in Appendix B.3, this voluntary restriction implies that this kind of protocols with decent security features are not considered private.

The Vaudenay and HPVP models are the most flexible ones since it is possible to choose either a NARROW or a WIDE adversary. Note that the other models can however be (more or less easily) adapted to provide both adversary classes.

12.3.2. Channels Asymmetry. As already explained in Section 3, the forward channel (reader to tag) has a longer communication range than the backward channel (tag to reader). This characteristic is of interest as it has been shown in [41] that the former can be more easily eavesdropped than the latter in practice. Yet, the Avoine model is the only one that formalizes this feature through the Execute* oracle: $\mathscr{A}$ may only obtain the messages sent by $\mathscr{R}$ on the forward channel.

All the other models (as a matter of fact, created after the Avoine one) lost this feature and cannot represent this kind of weaker but realistic adversary. Thus, assuming that $\mathscr{A}$ is only able to get the messages sent from $\mathscr{R}$, the analysis must be performed with the Avoine model.

12.3.3. Analyzable Protocols. Some models are designed "by default" to analyze specific identification/authentication protocols. In the Avoine model, the oracles to interact with the system can only be used for 3-pass protocols. Then, JW's authors only aim to analyze protocols based on symmetric-key cryptography. Finally, DLYZ can only analyze $(2\gamma + 1)$-pass protocols with $\gamma \geq 1$.

On the contrary, Vaudenay, LBM, DMR, CCEG, and HPVP can analyze any identification/authentication protocol. Some of the restrictive models can nevertheless be adapted to analyze most existing protocols. For instance, the Avoine model can be slightly modified to analyze 2-pass classical challenge-response protocols, and the JW model does not forbid the analysis of protocols with public-key cryptography.

Finally, considering protocols where the tag starts an execution, JW and DMR are the only models that are not restricted by default to analyze such protocols.

13. Privacy Properties

In the previous section, we discussed the features that are present (or not) in each of the studied models. To conclude the investigation, we go a step further and compare the privacy properties between them.

This task is not an easy one as the different features of each model make it tough to compare them in some cases. Indeed in the following section, we highlight the fact that, when a privacy property of a given model is said to be "stronger" than the one of another model, the "weaker" model may present some features that are not present in the "stronger" one. We assume that system designers are aware of this fact and that, in this special case, they may thus prefer to use the weaker model for their privacy analysis. Except when this fact must be highlighted, we will not detail it in each comparison.

13.1. Indistinguishability of Tags. Regarding only the privacy notions, the Avoine and JW models are really close. Indeed, they both define privacy as the unfeasibility for an adversary to recognize one tag among two. The JW model has been designed after the Avoine one, as an improved model since it takes into account several flaws of the Avoine model. It can be easily proved that JW's (ρ, σ, τ)-privacy (resp., forward-(ρ, σ, τ)-privacy) implies Avoine's Existential-UNT (resp., Forward-UNT): the goal is the same and any request of an Avoine's adversary can be performed by a JW's adversary.

In the DMR model, the privacy property corresponds to the unfeasibility to link two *traces* that are produced by the same agent (in our case, a tag). This notion is also really close to the one defined in the JW model. Clearly for JW, the adversary capacity to retrieve the tag associated to the bit b permits linking two traces and reciprocally. However, as the DMR model only defines a nonadaptive adversary regarding corruption, JW's (ρ, σ, τ)-privacy is obviously stronger than DMR's untraceability.

Largely inspired by the design of the Vaudenay model (on which we will come back later), the CCEG and HPVP models offer a comprehensive list of oracles that permit any JW's adversary to be represented in their models. Regarding the privacy definition, it is obvious that the output of a JW's adversary is exactly a CCEG's nonobvious link (*standard* or *past*) and can thus be directly exploited by a CCEG's adversary. As a consequence, CCEG's standard-untraceability (resp., past-untraceability) property obviously implies JW's (ρ, σ, τ)-privacy (resp., forward-(ρ, σ, τ)-privacy). The reciprocal does not lead to a tight reduction. Indeed, a CCEG's adversary may shuffle the tags' pseudonyms several times (by performing successive DrawTag and Free queries), which are hard to simulate in the JW model.

The HPVP model defines privacy using the well-known "left-or-right" paradigm. As detailed in Section 10, it splits the tags space into two worlds. Nevertheless, a JW's adversary can be simulated in this model. First the HPVP's adversary

draws each tag of the system. (A single tag can be given as the two inputs of the DrawTag oracle.) Then, the two selected challenge tags of JW are freed and given as input of the DrawTag oracle. If the JW's adversary is able to recognize the outputted tag, then it may be used by an HPVP's adversary to output the guessed bit. Here again, the reciprocal is not true for the same reasons as for the CCEG model.

As a conclusion, assuming that privacy is defined as indistinguishability of tags, the most comprehensive models are HPVP and CCEG. Intuitively, these two models have equivalent privacy notions. Indeed, an adversary that succeeds in the HPVP experiment can easily output a nonobvious link. On the opposite, a nonobvious link permits distinguishing one tag from the others and can thus be used in the "left-or-right" paradigm. However, it is not obvious to formally prove this equivalence result due to the following facts. Firstly, at one moment of the HPVP experiment, the adversary must use (at least once) the DrawTag oracle on two different tags in order to obtain information about the challenge bit. At that moment, this adversary can no longer interact with all the tags whereas a CCEG's adversary can always interact with all the tags if it wants to. Secondly, a CCEG's adversary may draw more than one tag in a DrawTag request (e.g., three tags out of four). If an HPVP's adversary wants to use such an adversary as a subroutine to succeed in the HPVP experiment, the simulation of this fact entails that some choices are mandatory and thus leads to a nontight reduction.

13.2. Real World versus Simulated World. The last three models (i.e., Vaudenay, LBM, and DLYZ) define privacy as, in a nutshell, the unfeasibility to distinguish the interactions of an adversary against the real system from the interactions of a simulated adversary against a simulated world. In this second world, the simulator does not know the keys of the system. Nevertheless, when a tag corruption is asked, the tag's real secret key is returned. The idea behind this privacy notion is that, if there exists a distinction between these two worlds, then some information must leak from the messages of the real world (which contains the real keys of the system).

The most adaptive and comprehensive model using this principle is clearly the Vaudenay model. First, this model offers the widest range of adversaries. Then, these adversaries can be adaptive, contrary to the ones of DLYZ. Finally, as explained in Section 12.1, the LBM model only ensures the privacy of authentications prior to the last complete one, while the Vaudenay model considers privacy of all the possible authentications. As a consequence, for equivalent adversary classes, the Vaudenay model is stronger than LBM and DLYZ.

From another point of view, the UC framework is generally used to analyze protocols that are not run alone, but in parallel/concurrency with other protocols. Here, the interesting feature is that the environment $\mathcal{Z}$ can interact with the system and thus may help $\mathcal{A}$ to perform its attack, while Vaudenay's adversary is on its own. This fact has been frequently used in the UC literature to prove that some "considered secure" constructions are indeed not. As a consequence, if the protocol to analyze is designed to belong to a complex system, its privacy may be studied in the LBM model. Nevertheless, if a strong privacy property is wished, the protocol should also be analyzed in the Vaudenay model.

13.3. Between the Two Families. The oracles description of the CCEG model is really close to the one of Vaudenay. The authors of the former describe their model as a restriction of the Vaudenay one, mainly on the experiment. Indeed, CCEG's adversary is required to output a nonobvious link, while any adversary assumption can be output in the Vaudenay model. Consequently, CCEG's privacy notion is intuitively weaker than Vaudenay's one (for equivalent adversary). Nevertheless, as proved in [11], CCEG's future-untraceability is a reachable property while Vaudenay's STRONG-privacy is impossible. Furthermore, to increase their result, CCEG's authors also prove with a "toy scheme" that their future-untraceability considers attacks that are not taken into account in the two "highest" reachable privacy levels of Vaudenay (i.e., the NARROW-STRONG and DESTRUCTIVE-privacy). As a consequence, the CCEG model defines a potentially weaker privacy notion, but, under this framework, protocol privacy can be studied against a stronger adversary than in the Vaudenay model.

Similar results may be proved for the HPVP model. First, its authors exhibit in their paper a protocol that ensures STRONG-privacy in their model. Then, using the "toy scheme" defined in [11], it can be proved that the same attacks (highlighted by CCEG) are also taken into account in HPVP's STRONG-privacy, which are again not considered in the reachable privacy levels of Vaudenay. However, as for the CCEG model, it can be proved that Vaudenay's privacy implies HPVP's one for equivalent adversary class. As this final result is not intuitive, we prove it in Appendix C.

To conclude this discussion, we highlight some existing results about the DLYZ model. The authors of the original paper argue that JW's (ρ, σ, τ)-privacy does not imply ZK-privacy and used several schemes to illustrate their claim. One example is a system composed of only one tag. Clearly, such a scheme cannot be analyzed in the JW model since it requires at least two tags in the experiment. Thus, their claim that the proposed scheme is (ρ, σ, τ)-private is doubtful. Additionally, the argument claiming that this scheme is not ZK-private is also not considered as acceptable, according to the authors of [42]. Furthermore, in such a special case of single-tag systems, DLYZ's authors say that ZK-privacy is reduced to the basic zero-knowledge definition which, according to them, provides a reasonable privacy. However in practice, each time this lonely tag is accepted by a reader, a WIDE adversary is obviously able to link this authentication to the previous ones. To our mind this is obviously a breach of privacy. Finally, the authors of [42] go one step beyond and formally prove that JW's (ρ, σ, τ)-privacy is equivalent to ZK-privacy (Theorem 1 of [42]).

14. Conclusion

In this paper, we first presented eight of the most well-known existing privacy models for RFID in details. We exhibited and

discussed the differences between these models regarding their features and their privacy notions. As a preliminary conclusion, none of the existing models encompass all the others. The first reason is that no model offers enough granularity to provide all the features detailed previously. Even if it is sometime possible to extend an existing model to take into account a new property or a new assumption, it is not always a trivial task to add all of them.

Throughout our study, it appears that the Vaudenay model is the one that integrates the greatest number of features and which defines the strongest privacy notion. As a default choice, the Vaudenay model is probably the best one. Nevertheless, some drawbacks have been highlighted. Firstly, the strongest privacy property of this model cannot be ensured by any protocol. To study the security of a protocol against the strongest (known) adversary, one may thus prefer the CCEG of the HPVP model. Secondly, the Vaudenay model (as other ones) considers that tracing a tag after an incomplete protocol execution compromises the privacy. On the one hand, this is a relevant consideration that ensures a strong privacy level. On the other hand, relaxing this constraint helps to design more efficient protocols with a still reasonable privacy level using the Avoine and LBM models. Finally, the lack of granularity of all the models involves difficulties to fairly distinguish, in a given model, protocols with different security levels.

If system designers have precisely defined the requested properties of their application and the assumptions regarding potential adversaries, then they might use our results to select the most appropriate model. Thereby, they can design or select the most adapted and efficient protocol for their needs. Nevertheless, we are convinced that unifying and simplifying the models would help the community to design and compare protocols meaningfully.

Appendices

A. General Statements about the UC Framework

A.1. The Environment $\mathcal{Z}$. In the UC framework, $\mathcal{Z}$'s purpose is to manage the evolution of the system $\mathcal{S}$. In other words, this entity is in charge of the activation of all the parties, including the adversary $\mathcal{A}$. $\mathcal{Z}$ is the only entity able to request a party $\mathcal{P}$ to initiate a new execution of the studied Ident protocol. It is also able to read the output tapes of the system and $\mathcal{A}$'s parties. On the other hand, $\mathcal{Z}$ is not assumed to read the incoming and outgoing messages of the parties during a protocol execution.

While this new entity is quite unusual compared to the other privacy models in RFID, it permits formalizing systems where there is an underlying communication structure which may be unknown to the adversary. In the other models, $\mathcal{A}$ is in charge of the activation of the parties. As a consequence, if there exists an underlying activation sequence that is unknown to the adversary, it cannot respect it and thus may lose information that would help it to perform its attack. The potential activation scheduling performed by $\mathcal{Z}$ thus strengthens the power of the adversary.

A.2. The Real World. The system $\mathcal{S}$ is composed of several *honest parties* that interact together through an Ident protocol in order to achieve a well-defined objective.

An adversary $\mathcal{A}$ is in charge of the communication channels: it can eavesdrop, modify, and schedule all the communication channels between the honest parties in an arbitrary way. $\mathcal{A}$ may also be able to corrupt parties and obtain the full knowledge of their state. Corrupted parties are assumed to be totally controlled by $\mathcal{A}$ afterwards.

$\mathcal{Z}$ and $\mathcal{A}$ can be discussed in an arbitrary way. Consequently, if $\mathcal{A}$ wants to, it can forward all the communications to $\mathcal{Z}$. It can also ask $\mathcal{Z}$ to launch new executions of Ident. At the end of the experiment, $\mathcal{A}$ may send its final output to $\mathcal{Z}$ which is the last activated entity of the system. Then, $\mathcal{Z}$ outputs an arbitrary string, denoted by $\text{EXEC}_{\text{Ident},\mathcal{A},\mathcal{Z}}$, which can be reduced to one bit as proved by Canetti in [31, 32].

A.3. The Ideal World. Here, all the honest parties have access to the *ideal functionality* $\mathcal{F}$, that is a trusted and uncorrupted party. $\mathcal{F}$ must trivially ensure the desired security objectives of the Ident protocol, and does not depend on any cryptographic mechanism.

Equivalently to the adversary $\mathcal{A}$ in the real world, a simulated adversary *Sim* is defined such that *Sim* can arbitrarily discuss with $\mathcal{Z}$. However, *Sim* can no longer directly interact with parties: it can only communicate with the ideal functionality $\mathcal{F}$ which manages all the entities' communications. The main goal of *Sim* is to reproduce the behavior of $\mathcal{A}$ in the real world as faithfully as possible. Since (i) $\mathcal{A}$ may transfer messages of the Ident protocol to $\mathcal{Z}$, (ii) *Sim* does not have access to Ident, and (iii) $\mathcal{F}$ does not produce such messages, then *Sim* should simulate these messages to $\mathcal{Z}$. The final output of $\mathcal{Z}$ is denoted by $\text{EXEC}_{\Phi,Sim,\mathcal{Z}}$, where the protocol Φ UC-realizes the ideal functionality $\mathcal{F}$ (as defined in [31]).

B. Detailed Privacy Analysis of Five Protocols

In the following, F and G refer to pseudorandom functions, while f and g refer to one-way functions. (Enc/Dec) refers to an encryption scheme. Finally, λ denotes the security parameter of the system.

B.1. SK-Based Challenge/Response Authentication Protocol [37]. In this protocol, it is obvious that one single corruption of a tag $\mathcal{T}$ allows it to be traced at any time. This is feasible as the secret key of a tag is a fixed value and the nonces used in the pseudorandom function are sent in the clear. Thus, an adversary is able to recompute the value E for the corrupted tag and compare it with the previously sent one. If these values are equal, then the adversary is convinced that the corrupted tag performed this authentication. (Note that this equality can be due to a collision, but this happens with a negligible probability.) Nevertheless, the corruption of another tag $\mathcal{T}'$ does not help to trace the tag $\mathcal{T}$, since all the secret keys are independent. Consequently, this protocol can only reach privacy properties when the adversary is not allowed to corrupt the challenge tags.

Therefore this protocol is Existential-UNT-RTE in the Avoine model (proved for this kind of protocols in [9]), and (ρ, σ, τ)-private in the JW model (proved in [16]). It is untraceable for DMR (proved in [13]) and ZK-private in the DLYZ model (the proof of a similar protocol in [12] can be trivially adapted).

This protocol is WEAK-private for Vaudenay (proved in [22]) and for HPVP. It is standard-untraceable for CCEG. The proofs for HPVP and CCEG are very similar to the ones of Vaudenay.

Finally, this protocol cannot UC-emulate the ideal functionality in the LBM model as the attack presented here permits an adversary to link several executions while this is not possible for the simulator (as $state(\mathcal{T})$ is removed after a corruption).

B.2. Tree-Based Authentication Protocol [8]. In this protocol, the main drawback is that some partial keys are shared by several tags. For instance, let us first say that a random tag $\mathcal{T}$ is chosen and corrupted: its secret keys $(k_0, k_{1,0}, k_{2,0}, \ldots)$ are revealed. Then, let us define the tags $\mathcal{T}_0$ and $\mathcal{T}_1$ as follows: $\mathcal{T}_0$'s keys are $(k_0, k_{1,0}, k_{2,0}, \ldots)$, and $\mathcal{T}_1$'s keys are $(k_0, k_{1,0}, k_{2,1}, \ldots)$. Clearly, $\mathcal{T}_0$ and $\mathcal{T}_1$ share the same path for the first two nodes, since they have the same keys for p_0 and p_1. But they have different keys for p_2. From the keys revealed during $\mathcal{T}$'s corruption, it is therefore possible to differentiate $\mathcal{T}_0$ and $\mathcal{T}_1$: $\mathcal{T}_0$'s answers will always be verifiable with $(k_0, k_{1,0}, k_{2,0})$, but this is not the case for $\mathcal{T}_1$ since it does not use the revealed key $k_{2,0}$. Note that, in the example, the challenge tags are not corrupted: only one other tag is corrupted.

Also, this protocol faces the same problem as the SK-based protocol: the corruption of a tag allows tracing it unconditionally. Thus for all the models, we consider that the adversary $\mathcal{A}$ is not allowed to corrupt (at least) the challenge tags. Note that this option is not available in LBM, and this protocol is consequently not forward-secure in this model.

It should not be possible to study this kind of protocols in the Avoine model because of the correlated secrets, but the analysis is given here to show the contrasts between the different models. Thus in the Avoine model, since $\mathcal{A}$ only plays with the two challenge tags, the protocol does not suffer from the previous attack. Therefore, the protocol is Existential-UNT-RTE (same proof as for the SK-based protocol). For Vaudenay and HPVP, the protocol is WEAK-private, and standard-untraceable for CCEG: clearly, since no secret is revealed, the proof is similar to the one for an SK-based protocol.

Then $\mathcal{A}$ is able to corrupt the nonchallenge tags in JW, and the tags that are not part of its attack in DMR. Thus, the attack presented above can be formalized in these two models. Consequently, the protocol is not (ρ, σ, τ)-private for JW (explained in [16] and proved in [6, 43]) and not untraceable for DMR.

For DLYZ, we use the method provided in [12] to show that the protocol is not ZK-private. We consider that *Sim* runs as subroutine the underlying adversary $\mathcal{A}$. Sim_1 just runs basically $\mathcal{A}_1$, and both adversaries obtain several keys from the corruption of nonclean tags in the first phase. Let us also consider that $\mathcal{A}_1$ and Sim_1 return a set C of clean tags where (i) $|C| \geq 2$ and (ii) each tag in C can be easily recognizable, thanks to the revealed keys. Then $\mathcal{A}_2$ will be able to recognize the challenge tag. But, Sim_2 does not know which challenge tag has been chosen. Thus Sim_2 has to choose at random a tag to simulate. At the end of the experiment, $\mathcal{A}$ will always retrieve the correct challenge tag, contrary to *Sim*: the views of $\mathcal{A}$ and *Sim* will be distinguishable. Therefore, the protocol is not ZK-private.

B.3. OSK-Based Authentication Protocol [22]. A significant attack on this kind of protocols has been defined by Juels and Weis in their privacy model [16], based on the fact that a tag's key can be updated while the equivalent one stored by the reader is not. Note that upon receipt of a message E, $\mathcal{R}$ tries to find a match with all tags' keys and their δ first updates. Thus, if the adversary $\mathcal{A}$ sends more than δ consecutive authentication requests to a tag without transferring the answers to $\mathcal{R}$, the shared secrets stored in $\mathcal{T}$ and $\mathcal{R}$ are consequently desynchronized. Therefore, if $\mathcal{A}$ has access to the authentication result on the reader's side, it is able to recognize a desynchronized tag $\mathcal{T}$ from another random tag as $\mathcal{T}$ will be rejected. This attack is generally called a *desynchronization attack*.

Recall that a NARROW adversary does not have access to the authentication result on the reader's side, while a WIDE one does have this access (e.g., through a Result query).

Considering a NARROW adversary, under the one-wayness assumption of g, it is obviously infeasible to link a secret key to a previous authentication transcript as this is equivalent to invert g. Furthermore, since all tags' secrets are independent, then corrupting one tag does not allow tracing the other ones. Since $\mathcal{A}$ is restricted to be NARROW in the Avoine and DMR models, the desynchronization attack does not work and thus the security level is equivalent to the one of the SK-based protocol (Figure 1), namely, the protocol is, respectively, Existential-UNT-RTE (proved in [9]) and untraceable (proof similar to the one in [13]). Considering tag corruption, it is furthermore Forward-UNT-RTEC in the Avoine model (proved in [9]). Regarding the Vaudenay and HPVP models, the protocol is NARROW-DESTRUCTIVE-private (proved in [15, 22]).

When $\mathcal{A}$ is WIDE, the protocol is vulnerable to the desynchronization attack explained above. Therefore, the protocol is not (ρ, σ, τ)-private for JW when $(\rho \geq 1, \sigma > \delta, \tau > \delta)$ (proved in [16]), and not standard-untraceable for CCEG. In the LBM model, a legitimate tag cannot be rejected in the ideal world as the ideal functionality will always accept it, while the desynchronization attack works in the real world.

For DLYZ, the same problem as for the tree-based protocol appears. If $|C| = 2$ and one of the two tags has been desynchronized by $\mathcal{A}_1$, then $\mathcal{A}_2$ can distinguish these tags depending on the result of an execution in the second phase. But Sim_2 does not know which challenge tag has been chosen. Thus Sim_2 has to choose at random a tag (victim or not of the desynchronization attack) to simulate. At the end of the experiment, $\mathcal{A}$ is always able to retrieve the correct challenge

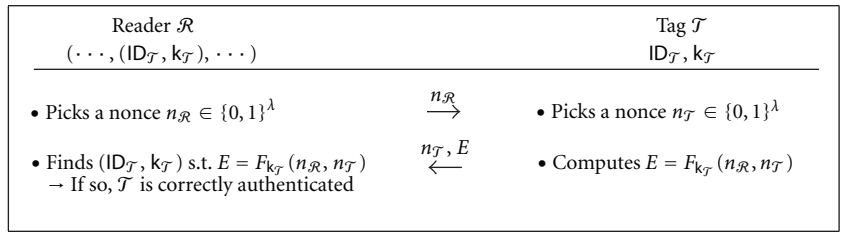


Figure 1: SK-based authentication protocol.

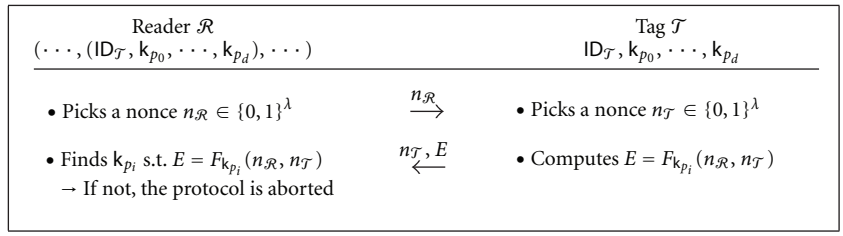


Figure 2: One round of the tree-based authentication protocol.

tag, which is not the case of *Sim*. This implies that the views of $\mathcal{A}$ and *Sim* will be distinguishable. Therefore, the protocol is not ZK-private, because at least one adversary can produce a distinguishable view (Figure 3).

B.4. O-FRAP Authentication Protocol [18]. The Search procedure is detailed in Algorithm 1 where Update($\mathcal{T}$) works as follows. First, if $\mathcal{R}$ uses $cur_{\mathcal{T}}$ to identify $\mathcal{T}$, then $\mathcal{R}$ replaces the content of $old_{\mathcal{T}}$ with the one of $cur_{\mathcal{T}}$. Secondly, $\mathcal{R}$ refreshes $cur_{\mathcal{T}} = (\mathsf{k}_{\mathcal{T}}^{cur}, n_{\mathcal{T}}^{cur})$ by (ν_4', ν_1').

Avoine et al. describe in [28] an attack which works when the adversary $\mathcal{A}$ is able to corrupt the challenge tag. This attack can be applied to the undesynchronizable protocols presented in [18, 24, 39]. First, $\mathcal{A}$ makes $\mathcal{T}$ and $\mathcal{R}$ start a new protocol execution, but $\mathcal{A}$ blocks the last message sent from $\mathcal{R}$ to $\mathcal{T}$. Then, if $\mathcal{A}$ corrupts $\mathcal{T}$ directly after this incomplete execution, it is able to recognize $\mathcal{T}$ by recomputing ν_2 as $\mathsf{k}_{\mathcal{T}}$ has not been updated and the nonces $(n_{\mathcal{R}}, n_{\mathcal{T}})$ have been sent in the clear. Note that the traceability attack of O-FRAP presented in [44] is specific to the way they define Algorithm 1 and does not apply here.

Therefore, no Corrupt query is allowed to an adversary of this protocol. In that case, the desynchronization attack of OSK does not work here. As a consequence, for JW, Vaudenay, CCEG, and HPVP, the privacy level of O-FRAP is the same as the one of the SK-based protocol (proofs are equivalent): it is, respectively, (ρ, σ, τ)-private, WEAK-private, standard-untraceable, and WEAK-private.

In the Avoine and DMR models, the protocol is Existential-UNT-RTE and untraceable: the attack presented above without corruption does not work since the tags' keys are needed. The proofs are thus similar to the ones of the SK-based protocol. The protocol is furthermore Forward-UNT-RTEC for Avoine, because, in that case, $\mathcal{C}$ can give $\mathcal{A}$ nonconsecutive intervals (contrary to the ones needed for the above attack): thus corrupting a tag does not help $\mathcal{A}$ to trace a tag.

Since the analysis for LBM is only related to completed protocol executions, this attack can be perfectly simulated in the ideal world using the knowledge of $active(\mathcal{T})$ as proved in [18]. The protocol is thus forward-secure.

For DLYZ, the protocol is ZK-private: the proof is similar to the one of the SK-based protocol when no corruption is allowed. Regarding the forward-ZK-privacy, it is possible to define an adversary $\mathcal{A}$ that has a distinguishable view than the simulator's one. Let us consider that $|C| \geq 2$. Sim_1 just runs $\mathcal{A}_1$ as subroutine. Then $\mathcal{A}_2$ forces an interaction between $\mathcal{R}$ and $\mathcal{T}_c$ and blocks the last message. Sim_2 has to provide a simulated incomplete interaction of $\mathcal{R}$ with $\mathcal{T}_c$: since Sim_2 does not have any information about $\mathcal{T}_c$, this interaction can only be composed of random messages. At the end, $\mathcal{T}_c$'s secrets are revealed to a distinguisher $\mathcal{D}$. Thus $\mathcal{D}$ is able to recognize if $\mathcal{A}_2$'s interaction corresponds to a real incomplete interaction with $\mathcal{T}_c$ or a simulated one. The protocol is therefore not forward-ZK-private (Figure 4).

B.5. PK-Based Challenge/Response Authentication Protocol [22]. First, it is important to note that, under IND-CPA security, this protocol may not be easily proved private for WIDE adversaries in any model. The main reason is that the simulator/blinder in the proof does not have access to a decryption oracle in the IND-CPA experiment. Therefore, this simulator/blinder is unable to correctly simulate the Result oracle and thus has to answer at random 0 or 1 in some cases. Here, an adversary $\mathcal{A}$ may be able to detect if it is interacting with the real world or with a simulated one. CCEG proves that standard-untraceability can nevertheless be reached by PK-based protocols using IND-CPA cryptosystem but by adding other security mechanisms to the protocol (i.e., a MAC scheme).

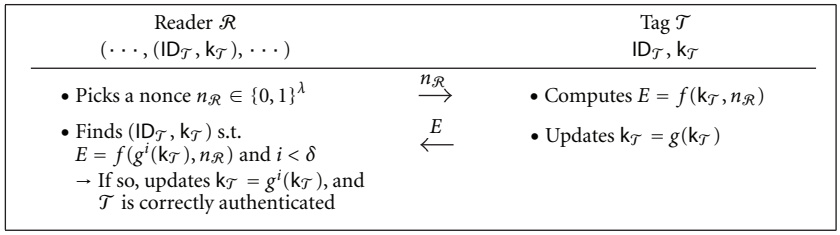


Figure 3: OSK-based authentication protocol.

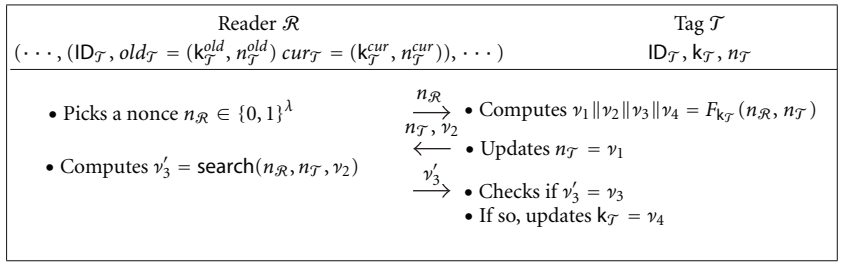


Figure 4: O-FRAP authentication protocol.

Input: $n_{\mathcal{R}}'; n_{\mathcal{T}}, \nu_2$
Output: ν_3
(1) $Out \longleftarrow \perp$
(2) **if** $\exists$ $(\mathrm{ID}_{\mathcal{T}}, old_{\mathcal{T}}', cur_{\mathcal{T}}')$ s.t. $n_{\mathcal{T}} = n_{\mathcal{T}}^{old}$ (resp. $n_{\mathcal{T}} = n_{\mathcal{T}}^{\mathrm{cur}}$) **then**
(3) $\quad \nu_1' \| \nu_2' \| \nu_3' \| \nu_4' \longleftarrow F_{\mathsf{k}_{\mathcal{T}}^{old}}(n_{\mathcal{R}}, n_{\mathcal{T}}^{old})$ (resp. $\nu_1' \| \nu_2' \| \nu_3' \| \nu_4' \longleftarrow F_{\mathsf{k}_{\mathcal{T}}^{cur}}(n_{\mathcal{R}}, n_{\mathcal{T}}^{cur})$)
(4) $\quad$ **if** $\nu_2' = \nu_2$ **then**
(5) $\quad\quad \mathcal{T}$ is correctly authenticated
(6) $\quad\quad Out \longleftarrow \nu_3'$
(7) $\quad\quad \mathsf{Update}\ (\mathcal{T})$
(8) $\quad$ **end if**
(9) **end if**
(10) **for all** $(\mathrm{ID}_{\mathcal{T}}, old_{\mathcal{T}}', cur_{\mathcal{T}}')$ **and** $c \varepsilon \{old_{\mathcal{T}}, cur_{\mathcal{T}}\}$ **do**
(11) $\quad \nu_1' \| \nu_2' \| \nu_3' \| \nu_4' \longleftarrow F_{\mathsf{k}_{\mathcal{T}}^{c}}(n_{\mathcal{R}}, n_{\mathcal{T}})$
(12) $\quad$ **if** $\nu_2' = \nu_2$ **then**
(13) $\quad\quad \mathcal{T}$ is correctly authenticated
(14) $\quad\quad Out \longleftarrow \nu_3'$
(15) $\quad\quad \mathsf{Update}\ (\mathcal{T})$
(16) $\quad$ **end if**
(17) **end for**
(18) **return** Out

Algorithm 1: The search procedure.

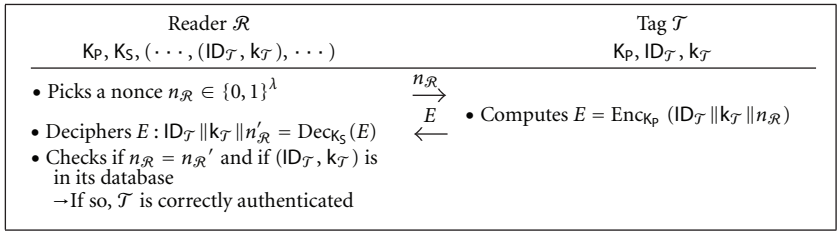


Figure 5: PK-based authentication protocol.

For Avoine and DMR, since $\mathcal{A}$ is NARROW, this problem does not appear (i.e., no query to RESULT). When the cryptosystem is IND-CPA secure, the protocol is thus Existential-UNT-RTE and Forward-UNT-RTEC for Avoine, and untraceable for DMR.

The proof is as follows in the Avoine model but can be easily adapted for the DMR model. We show that, if there exists an adversary $\mathcal{A}$ that wins $\mathrm{Exp}^{P\text{-UNT}}_{\mathcal{S},\mathcal{A}}$ (with $P \in \{\mathsf{Existential}, \mathsf{Forward}\}$), then it is possible to construct an adversary $\mathcal{A}'$ that wins the IND-CPA game. To do so, $\mathcal{A}'$ runs $\mathcal{A}$ as subroutine, simulating the system $\mathcal{S}$ to $\mathcal{A}$ by answering all oracles queries made by $\mathcal{A}$. At the end of the IND-CPA game, $\mathcal{A}'$ answers what $\mathcal{A}$ answers for $\mathrm{Exp}^{P\text{-UNT}}_{\mathcal{S},\mathcal{A}}$. Here, $\mathcal{A}'$ knows the secrets of $\mathcal{T}_0$ and $\mathcal{T}_1$ at the beginning of the IND-CPA game, in order to perform it. When $\mathcal{A}$ asks the interactions for $\mathcal{T}_0$ and $\mathcal{T}_1$, $\mathcal{A}'$ answers the corresponding ciphertexts for these interactions using the correct plaintext. When $\mathcal{A}$ asks the interactions for $\mathcal{T}$, then $\mathcal{A}'$ submits the plaintexts for both $\mathcal{T}_0$ and $\mathcal{T}_1$ for these interactions to the IND-CPA challenger $\mathcal{C}'$. $\mathcal{A}'$ receives the ciphertexts answered by $\mathcal{C}'$ for $\mathcal{T}_b$, where b is the unknown bit of the IND-CPA experiment, and transfers them to $\mathcal{A}$. So far, the simulation done by $\mathcal{A}'$ to $\mathcal{A}$ is perfect. Then, two cases can occur.

(1) $\mathcal{A}$ does not need $\mathcal{T}$'s secrets (i.e., $\mathcal{A}$ is playing the Existential experiment). $\mathcal{A}$ wins $\mathrm{Exp}^{\mathsf{Existential\text{-}UNT}}_{\mathcal{S},\mathcal{A}}$, thus its advantage is nonnegligible, so is the advantage of $\mathcal{A}'$.

(2) $\mathcal{A}$ asks $\mathcal{T}$'s secrets (i.e., $\mathcal{A}$ is playing the Forward experiment). $\mathcal{A}'$ does not know b, thus it sends at random $\mathcal{T}_0$'s or $\mathcal{T}_1$'s secrets. If $\mathcal{A}'$ sends the expected ones, then $\mathcal{A}$ wins $\mathrm{Exp}^{\mathsf{Forward\text{-}UNT}}_{\mathcal{S},\mathcal{A}}$, thus its advantage is nonnegligible, so is the advantage of $\mathcal{A}'$. If not, at worst $\mathcal{A}$ answers at random 0 or 1. Therefore, the whole advantage of $\mathcal{A}$ is nonnegligible, so is the advantage of $\mathcal{A}'$.

Consequently, $\mathcal{A}'$ is an adversary that wins the IND-CPA game with nonnegligible advantage, which concludes the proof.

Vaudenay proves in [22] that the protocol is NARROW-STRONG-private with IND-CPA security and that it is furthermore FORWARD-private with IND-CCA. Since the privacy notions of JW are included in Vaudenay (as explained in Section 13), the protocol is thus forward-(ρ, σ, τ)-private for JW. HPVP proves in [15] that the protocol is also NARROW-STRONG-private with IND-CPA security but that it is STRONG-private with IND-CCA.

In the LBM model, if an environment is able to distinguish the real world from the ideal one, it can easily be transformed into a distinguisher of the IND-CCA property of the underlying encryption scheme. Thus it is obvious that this protocol is forward-secure.

In the CCEG model, the protocol is future-untraceable with IND-CCA security (proved in [11]). In the DLYZ model, the protocol is also backward-ZK-private with IND-CCA security: the proof follows the same reasoning as the one of CCEG (Figure 5).

C. The Vaudenay Model Implies the HPVP Model

The following theorem proves that, for a given adversary class, the privacy property of the Vaudenay model is at least stronger than the one of HPVP.

Theorem 19. *For any adversary class* $P \in \{\varnothing, \mathsf{NARROW}\} \times \{\mathsf{WEAK}, \mathsf{FORWARD}, \mathsf{DESTRUCTIVE}, \mathsf{STRONG}\}$, *then the P-privacy property of the Vaudenay model implies the P-privacy property of the HPVP model.*

Proof. Both models define the same adversary classes but differ in their experiment. However, we show here that, for a given class P, Vaudenay's P-privacy implies HPVP's one. To do so, we exhibit an adversary in Vaudenay, denoted $\mathcal{A}_{\mathsf{Vaud}}$, that emulates the system to an adversary playing the HPVP's P-experiment, denoted $\mathcal{A}_{\mathsf{HPVP}}$, and uses the output of the latter to break Vaudenay's P-privacy.

First, $\mathcal{A}_{\mathsf{Vaud}}$ can answer all the possible queries performed by $\mathcal{A}_{\mathsf{HPVP}}$ during its experiment. The SENDTAG, SENDREADER, RESULT, CREATETAG, and LAUNCH queries can be easily emulated by $\mathcal{A}_{\mathsf{Vaud}}$ due to their large similarity. For the DRAWTAG oracle, the Vaudenay model should be slightly modified in order to emulate the one of HPVP. Indeed in HPVP, this oracle formalizes the "left-or-right" paradigm. To handle this issue, we assume that, when $\mathcal{A}_{\mathsf{Vaud}}$ gives as input of DRAWTAG a probability distribution with the form "$\Pr[\mathsf{ID}_i] = 1/2, \Pr[\mathsf{ID}_j] = 1/2$," then this also follows the "left-or-right" paradigm as well.

Also, $\mathcal{A}_{\mathsf{HPVP}}$ can only corrupt free tags while only drawn tags can be corrupted in the Vaudenay model. Nevertheless, $\mathcal{A}_{\mathsf{Vaud}}$ can correctly reply to these queries: upon a corruption query of the tag $\mathcal{T}$, $\mathcal{A}_{\mathsf{Vaud}}$ draws $\mathcal{T}$ using a special distribution probability which attribute a probability of 1 to $\mathcal{T}$ and 0 for all the other tags. Then, it can corrupt it, transmits the data to $\mathcal{A}_{\mathsf{HPVP}}$, and then frees $\mathcal{T}$. This method correctly works for DESTRUCTIVE and STRONG adversaries (and their NARROW variants). However, it must be adapted for a FORWARD adversary. Indeed, in both models, such an adversary can only perform corrupt queries after that the first one has been made, and $\mathcal{A}_{\mathsf{Vaud}}$ must anticipate all these possible queries of $\mathcal{A}_{\mathsf{HPVP}}$. Thus, upon the first corruption query, $\mathcal{A}_{\mathsf{Vaud}}$ first frees all tags and then draws them one by one in order to know the correspondences between all the tags identifiers and their pseudonyms. Finally, $\mathcal{A}_{\mathsf{Vaud}}$ is able to reply to all the corruption queries correctly.

This simulation is perfect and cannot be detected by $\mathcal{A}_{\mathsf{HPVP}}$ that, as a consequence, will output its guessed bit b' with its habitual probability. Then, using this bit, $\mathcal{A}_{\mathsf{Vaud}}$ can decide which tag has been drawn by the DRAWTAG queries. Therefore, the success probability of $\mathcal{A}_{\mathsf{Vaud}}$ is exactly the one

of $\mathcal{A}_{\mathsf{HPVP}}$. As Vaudenay's blinder cannot decide in advance which tag should be simulated after a DrawTag, the success probability of this blinded adversary is necessary one half (random guess of the bit).

Thus, if there exists an attack for a given system against the P-privacy in HPVP, then there exists an attack against the P-privacy that succeeds with the same probability in the Vaudenay model. Therefore, for any adversary class P, Vaudenay's P-privacy implies HPVP's one. □

The reciprocal is hard to prove for two main reasons. Firstly, Vaudenay's experiment output is not specified and may thus be unexploitable by $\mathcal{A}_{\mathsf{HPVP}}$. Secondly, the DrawTag oracle may receive as input an arbitrary distribution that can be hard to simulate using the "left-or-right" DrawTag of HPVP.

Acknowledgment

This work was partially funded by the Walloon Region Marshall plan through the 816922 Project SEE.

References

[1] EPCglobal. Class-1 Generation 2 UHF Air Interface Protocol Standard Version 1. 2. 0: Gen 2, 2008, http://www .epcglobal-inc.org/standards/.

[2] Infineon, Contactless SLE 66 Family, http://www.infineon .com/.

[3] NXP Semiconductors, DESFire Tags, http://www.nxp.com/.

[4] A. Cavoukian, Privacy-by-Design, http://privacybydesign.ca/.

[5] Viviane Reding. Commission recommendation of 12. 05. 2009—SEC(2009) 585/586, on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, 2009.

[6] G. Avoine, E. Dysli, and P. Oechslin, "Reducing time complexity in RFID systems," in *Proceedings of the 12th International Conference on Selected Areas in Cryptography (SAC '05)*, vol. 3897 of *Lecture Notes in Computer Science*, pp. 291–306, Springer, Kingston, Canada, 2005.

[7] G. Avoine and P. Oechslin, "A scalable and provably secure hash-based RFID protocol," in *Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW '05) Workshops*, pp. 110–114, IEEE, Kauai Island, Hawaii, USA, March 2005.

[8] D. Molnar and D. Wagner, "Privacy and security in library RFID issues, practices, and architectures," in *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*, pp. 210–219, ACM, Washington, DC, USA, October 2004.

[9] G. Avoine, "Adversary model for radio frequency identification," LASEC-REPORT 2005-001, Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC), Lausanne, Switzerland, 2005.

[10] M. Burmester, T. van Le, B. de Medeiros, and G. Tsudik, "Universally composable RFID identification and authentication protocols," *ACM Transactions on Information and System Security*, vol. 12, no. 4, article 21, 2009.

[11] S. Canard, I. Coisel, J. Etrog, and M. Girault, "Privacy-preserving RFID systems: model and constructions," Cryptology ePrint Archive, Report 2010/405, 2010.

[12] R. H. Deng, Y. Li, M. Yung, and Y. Zhao, "A new framework for RFID Privacy," in *Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS '10)*, vol. 6345 of *Lecture Notes in Computer Science*, pp. 1–18, Springer, Athens, Greece, 2010.

[13] T. van Deursen, S. Mauw, and S. Radomirović, "Untraceability of RFID protocols," in *Proceedings of the 2nd IFIP WG 11.2 International Conference on Information Security Theory and Practices: Smart Devices, Convergence and Next Generation Networks (WISTP '08)*, vol. 5019 of *Lecture Notes in Computer Science*, pp. 1–15, Springer, Sevilla, Spain, May 2008.

[14] J.-H. Ha, S.-J. Moon, J. Zhou, and J.-C. Ha, "A new formal proof model for RFID location privacy," in *Proceedings of the 13th European Symposium on Research in Computer Security (ESORICS '08)*, vol. 5283 of *Lecture Notes in Computer Science*, pp. 267–281, Springer, Malaga, Spain, 2008.

[15] J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel, "A new RFID privacy model," in *Proceedings of the 16th European Symposium on Research in Computer Security (ESORICS '11)*, vol. 6879 of *Lecture Notes in Computer Science*, pp. 568–587, Springer, Leuven, Belgium, 2011.

[16] A. Juels and S. A. Weis, "Defining strong privacy for RFID," in *Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom '07)*, pp. 342–347, IEEE, New York, NY, USA, March 2007.

[17] J. Lai, R. H. Deng, and Y. Li, "Revisiting unpredictability-based RFID privacy models," in *Proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS '10)*, vol. 6123 of *Lecture Notes in Computer Science*, pp. 475–492, Springer, Beijing, China, 2010.

[18] T. van Le, M. Burmester, and B. de Medeiros, "Universally composable and forward-secure RFID authentication and authenticated key exchange," in *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS '07)*, pp. 242–252, ACM, Singapore, March 2007.

[19] C. Ma, Y. Li, R. H. Deng, and T. Li, "RFID privacy: relation between two notions, minimal condition, and efficient construction," in *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*, pp. 54–65, ACM, Chicago, Ill, USA, November 2009.

[20] K. Ouafi, *Security and privacy in RFID systems [Ph.D. thesis]*, EPFL, Lausanne, Switzerland, 2011.

[21] R.-I. Paise and S. Vaudenay, "Mutual authentication in RFID: security and privacy," in *Proceedings of the 3rd ACM Symposium on Information, Computer and Communications Security (ASIACCS '08)*, pp. 292–299, ACM, Tokyo, Japan, March 2008.

[22] S. Vaudenay, "On privacy models for RFID," in *Proceedings of 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '07)*, vol. 4833 of *Lecture Notes in Computer Science*, pp. 68–87, Springer, Kuching, Malaysia, December 2007.

[23] C. Su, Y. Li, Y. Zhao, R. H. Deng, Y. Zhao, and J. Zhou, "A survey on privacy frameworks for RFID authentication," *IEICE Transactions on Information and Systems*, vol. 95, no. 1, pp. 2–11, 2012.

[24] S. Canard and I. Coisel, "Data synchronization in privacy-preserving RFID authentication schemes," in *Proceedings of the 4th Workshop on RFID Security (RFIDSec '08)*, Budapest, Hungary, July 2008.

[25] S. Bocchetti, *Security and privacy in RFID protocols [M.S. thesis]*, Università degli Studi di Napoli Federico II, Naples, Italy, 2006.

[26] F. Armknecht, A. R. Sadeghi, A. Scafuro, I. Visconti, and C. Wachsmann, "Impossibility results for RFID privacy notions,"

Transaction on Computational Science XI, vol. 6480, pp. 39–63, 2010.

[27] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes," in *Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '98)*, vol. 1462 of *Lecture Notes in Computer Science*, pp. 26–45, Springer, Santa Barbara, Calif, USA, 1998.

[28] G. Avoine, I. Coisel, and T. Martin, "Time measurement threatens privacy-friendly RFID authentication protocols," in *Proceedings of the 6th International Conference on Radio Frequency Identification: Security and Privacy Issues (RFIDSec '10)*, vol. 6370 of *Lecture Notes in Computer Science*, pp. 138–157, Springer, Istanbul, Turkey, 2010.

[29] P. D'Arco, A. Scafuro, and I. Visconti, "Revisiting DoS attacks and privacy in RFID-enabled networks," in *Proceedings of the 5th International Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS '09)*, vol. 5804 of *Lecture Notes in Computer Science*, pp. 76–87, Springer, Rhodes, Greece, 2009.

[30] F. D. Garcia and P. van Rossum, "Modeling privacy for off-line RFID systems," in *Proceedings of the 9th Smart Card Research and Advanced Applications (CARDIS '10)*, vol. 6035 of *Lecture Notes in Computer Science*, pp. 194–208, Springer, Passau, Germany, 2010.

[31] R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," Cryptology ePrint Archive, Report 2000/067, 2000.

[32] R. Canetti, "Security and Composition of Cryptographic Protocols: A Tutorial," Cryptology ePrint Archive, Report 2006/465, 2006.

[33] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[34] F. D. Garcia, I. Hasuo, W. Pieters, and P. van Rossum, "Provable anonymity," in *ACM Workshop on Formal Methods in Security Engineering (FMSE '05)*, pp. 63–72, ACM, Alexandria, VA, USA, November 2005.

[35] S. Mauw, J. H. S. Verschuren, and E. P. de Vink, "A formalization of anonymity and onion routing," in *Proceedings of the 9th European Symposium on Research in Computer Security (ESORICS '04)*, vol. 3193 of *Lecture Notes in Computer Science*, pp. 109–124, Springer, Sophia Antipolis, France, 2004.

[36] S. Canard, I. Coisel, and M. Girault, "Security of privacy-preserving RFID systems," in *Proceedings of IEEE International Conference on RFID-Technology and Applications (RFID-TA '10)*, pp. 269–274, IEEE, Guangzhou, China, June 2010.

[37] International Organization for Standardization, ISO/IEC, 9798: Information technology—Security techniques—Entity authentication, 1991–2010.

[38] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to "privacy-friendly" tags," in *RFID Privacy Workshop*, MIT, Cambridge, Mass, USA, November 2003.

[39] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm '05)*, pp. 59–66, IEEE, Athens, Greece, September 2005.

[40] T. van Deursen, *Security of RFID protocols [Ph.D. thesis]*, University of Luxembourg, Walferdange, Luxembourg, 2011.

[41] G. P. Hancke, "Practical eavesdropping and skimming attacks on high-frequency RFID tokens," *Journal of Computer Security*, vol. 19, no. 2, pp. 259–288, 2011.

[42] D. Moriyama, S. Matsuo, and M. Ohkubo, "Relation among the security models for RFID authentication protocol," in *ECRYPT Workshop on Lightweight Cryptography*, Louvain-la-Neuve, Belgium, 2011.

[43] G. Avoine, B. Martin, and T. Martin, "Tree-based RFID authentication protocols are definitively not privacy-friendly," in *Proceedings of the 6th International Conference on Radio Frequency Identification: Security and Privacy Issues (RFIDSec '10)*, vol. 6370 of *Lecture Notes in Computer Science*, pp. 103–122, Springer, Istanbul, Turkey, 2010.

[44] K. Ouafi and R. C. W. Phan, "Traceable privacy of recent provably-secure RFID protocols," in *Proceedings of the 6th International Conference on Applied Cryptography and Network Security (ACNS '08)*, vol. 5037 of *Lecture Notes in Computer Science*, pp. 479–489, Springer, New York City, NY, USA, June 2008.

Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2013, Article ID 392056, 19 pages
http://dx.doi.org/10.1155/2013/392056

Research Article

Wireless Sensing Based on RFID and Capacitive Technologies for Safety in Marble Industry Process Control

Fabrizio Iacopetti, Sergio Saponara, Luca Fanucci, and Bruno Neri

Department of Information Engineering, University of Pisa, Via Caruso 16, 56122 Pisa, Italy

Correspondence should be addressed to Fabrizio Iacopetti; fabrizio.iacopetti@iet.unipi.it

Received 29 July 2012; Accepted 19 October 2012

Academic Editor: Agusti Solanas

This paper presents wireless sensing systems to increase safety and robustness in industrial process control, particularly in industrial machines for marble slab working. The process is performed by abrasive or cutting heads activated independently by the machine controller when the slab, transported on a conveyer belt, is under them. Current slab detection systems are based on electromechanical or optical devices at the machine entrance stage, suffering from deterioration and from the harsh environment. Slab displacement or break inside the machine due to the working stress may result in safety issues and damages to the conveyer belt due to incorrect driving of the working tools. The experimented contactless sensing techniques are based on four RFID and two capacitive sensing technologies and on customized hardware/software. The proposed solutions aim at overcoming some limitations of current state-of-the-art detection systems, allowing for reliable slab detection, outside and/or inside the machine, while maintaining low complexity and at the same time robustness to industrial harsh conditions. The proposed sensing devices may implement a wireless or wired sensor network feeding detection data to the machine controller. Data integrity check and process control algorithms have to be implemented for the safety and reliability of the overall industrial process.

1. Introduction

The transformation of stone blocks coming from quarries into finished products, for example, tiles, sculptures, building materials, stone powder, and so forth, is performed through several different industrial processes. In the case of slab-shaped products (e.g., tiles), marble blocks coming from quarries are firstly sawn by a gangsaw [1] into marble slabs with a resulting irregular contour and with rough surfaces. Slabs are afterwards polished in a polishing machine [2], cut into smaller and regular slabs by means of cutting machines, and finally become end products. The process control of marble slab working is nowadays mainly based on a feed-forward control scheme: the marble slab is transported inside the machine by a conveyer belt; at the entrance of the machine, contact or optical sensing technologies are used to derive information on the presence and shape of the slab which are then used by the machine controlling system to drive the working heads on the slab when it is passing under them. Due to unforeseen events that may occur to the slab inside the machine, mainly slab displacement and cracks, the controlling system may drive the working heads on the base of not up-to-date or wrong information on the shape and position of the slab. This leads to damages for the machine, in particular for the conveyer belt, with resulting costs due to the need of replacing damaged parts and above all to the machine stop. The detection of slab cracks and of other working problems is nowadays still demanded to operators supervising the machine during the course of the working, who stop the machine in case of suspected or occurred problems. This approach may result in late intervention and in consequent machine damages but also may increase the safety risks for the workers. Moreover, the currently industrially used slab sensing technologies suffer from some issues like deterioration and performance problem in the dirty and wet working environment (mud, water, and stone residuals).

For the above-mentioned reasons, a feedback control scheme on the slab position inside the machine would turn into an improvement for the reliability and safety of the industrial process control.

This paper deals in particular with the use of contactless sensing technologies, specifically based on RFID (radio frequency identification) and capacitive techniques, and to a multipoint wireless sensing data generation approach to improve the reliability and safety in industrial machines for marble slabs polishing. The proposed approach can be generally applied to other machines for stone slab working (cutting, waxing, etc.). The use of wireless technologies in industrial applications is an interesting and emerging trend, aiming at reducing cabling and installation complexity and costs and at avoiding the danger of cables and connectors failure especially on moving parts of industrial machines. Several works have been proposed in the literature [3] mainly addressing wireless systems for industrial communication or, in the case of RFID techniques, for positioning and logistics. On the contrary this work exploits RFID wireless technologies both for contactless multipoint sensing and wireless data communication; the work proposes and examines also the use of multipoint capacitive sensing techniques. For both RFID- and capacitive-based sensing applications, hardware and software components have been developed or COTS (commercial off the shelf) devices have been characterized and proposed for an integration within the machine process control architecture. This approach is supported by experimental campaigns on sensor performance using both sensing wireless technologies (RFID and capacitive) and considering working environments representative of those found in real industrial applications.

After this introduction this work briefly reviews in Section 2 the working principle of industrial marble machines and the state-of-the-art solutions based on optical and mechanical sensors and their limits. Section 3 introduces 4 RFID systems analyzed and tested in the present work, each one based on a different RFID technology, to try overcoming through contactless and wireless sensing the limits of the state-of-the-art process control applications. Then, in Section 4 to 7, the work presents the applications and results concerning the test of the 4 mentioned RFID technologies applied to the case of slab detection in conditions representative of a real industrial working scenario. Section 8 presents the basic principle for capacitive sensing (capacitive sensor and the relevant front-end acquisition circuitry), while Section 9 presents two different types of capacitive sensors that have been designed, implemented, and tested in a test setup representative of real industrial working conditions. A comparison among the different analyzed contactless and wireless sensing solutions, based on RFID and capacitive technologies, is reported in Section 10. Conclusions are drawn in Section 11.

2. Process Control and Sensors in Industrial Marble Machines

Figure 1 shows the schematic diagram of a typical industrial marble machine for slab working. Marble machines are typically made up of consecutive working heads (up to a few tens) under which the marble slab, initially brought to the machine by means of a roller system, is transported by a plastic conveyer belt [2]. A marble slab is typically sized 2 m × 3 m and has a thickness of some cm. The typical conveyer belt speed amounts to a few cm/s. As an example, the polishing machine in [2] has a total length of 13.5 m and up to 18 abrasive heads.

In Figure 2 the schematic illustration of a section constituted by the different materials/parts inside the machine is reported.

The working environment inside a marble machine is dirty, due to mud, marble, and abrasive residuals, and wet, due to a water level of few cm needed for heads cooling, elimination of residuals, and easing of the conveyer belt sliding on the machine metallic plane. These mentioned issues add up to the other classic problems of wireless systems in industrial scenarios, such as electromagnetic signal attenuation, multipath, and interference from other electromagnetic sources like electrical motors.

As mentioned in Section 1, the process control for marble slab working is currently based on the following scheme: mechanical or optical sensors, arranged in a linear array at the entrance of the machine, are sampled at regular intervals (i.e., each second) to detect the presence of the marble slab on the conveyer belt at the entrance of the industrial machine (profile reader in Figure 1). Such approach results in a spatial sampling of the slab area, with sample step of a few cm, which is used by the PLC (programmable logic controller) controlling the entire machine, including the conveyer belt speed, as the reference time to drive down each cutting/abrasive head when the marble slab is available and to drive up the head in the initial position when the slab is overpassing the working tool. The above-mentioned feed-forward control rule is based on the assumptions that the position and speed of the conveyer belt, the position of the marble slab on the belt, and therefore the relative positions of the heads are constantly known. If one of such assumptions is not verified, in particular the position of the slab on the belt, then the marble slab may not be present when the head is driven down, so that the latter reaches and damages the conveyer belt which must be repaired or replaced causing a long stop of the machine and of the industrial production. During the long travel inside the machine, the slab might indeed move on the conveyer belt due to the working forces or due to breaks under the working mechanical stress. Hence a feedback detection signal should be provided to the heads control system about the real presence of the marble slab under the head inside the machine.

In addition to the missing feedback to the heads control system inside the machine, the state-of-the-art sensors for slab detection outside the machine have problems still to overcome: mechanical sensors suffer from deterioration due to the continuous contact with the slab, while optical sensors [4] need frequent cleaning and recalibration due to the dirty working environment; see Figure 3.

Due to the wet and dirty working conditions and to the nonhomogeneous and nonconstant environmental physical properties, also other contactless sensors proposed or potentially suitable for marble machines, based on LASER or vision systems or ultrasonic waves [5–8], turned out not to be suitable for successful industrial applications.

Capacitive sensors for marble [9] and more complex ultrasound- or georadar-based systems [6, 8, 10] have been studied in the literature. However, their target is the

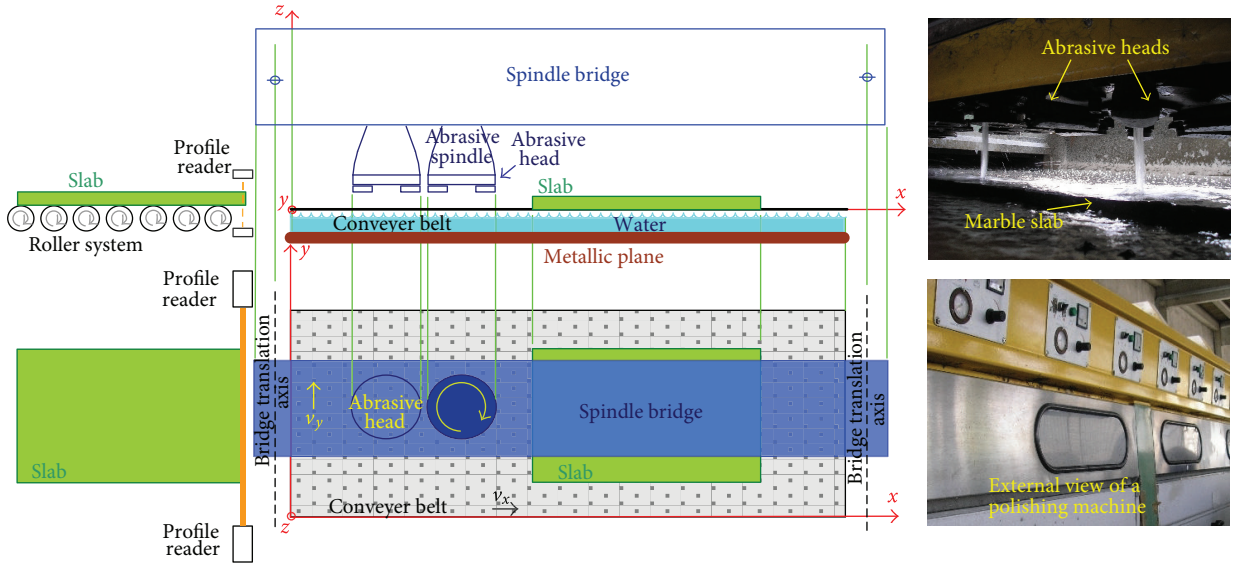


FIGURE 1: Schematic diagram of a marble machine and a snapshot of the abrasive heads over a marble slab.

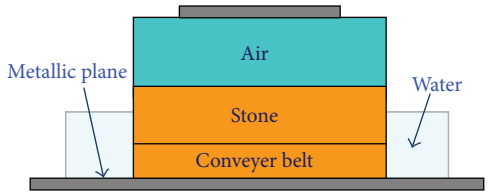


FIGURE 2: Schematic representation of a section of the different materials/parts inside the machine.

fine-grain analysis of the porosity and defects of stone materials (e.g., measuring the dielectric permittivity variations) in a controlled working environment (dry, clean, and with still stone samples) rather than the real-time detection of the presence of a marble slab during the working process inside an industrial machine.

In [11] we have presented preliminary results from experimental tests exploiting capacitive sensing for the detection of the marble slab at the entrance and inside the marble machine, which are further illustrated in Sections 9.1 and 9.2.

Proximity capacitive sensors have also been proposed by semiconductor industry in [12] but targeting small distances mainly for touch sensing applications.

Marble detection through RFID systems, exploiting the interaction between stones and RF radiations, has been preliminary discussed by us in [13] and will be further detailed in the following Section 3 to Section 8.

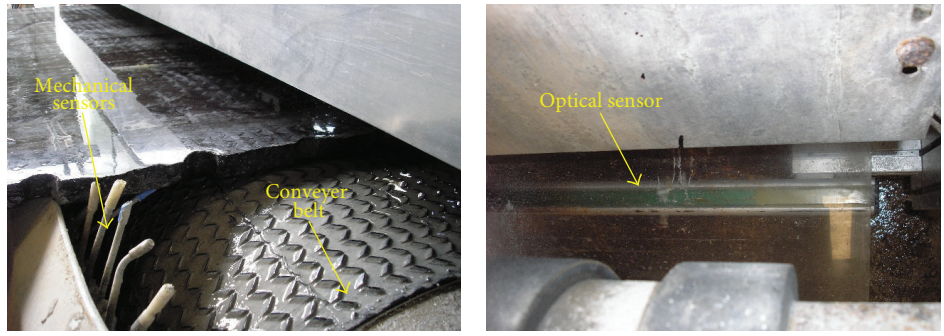
Also the techniques proposed in [5–8, 14, 15] aim at classification and fine-grain analysis of the texture and surface of stone slabs in a static and controlled environment, with conditions different from those found inside a marble machine. Moreover, for marble machines a simpler on/off detection is required, but with the possibility to be performed in real time, with higher robustness, to be easily integrated with the machine controlling system, having low maintenance costs. Finally, the computational power needed to implement computing techniques based on wavelets, Gabor filters, or neural networks as in [6, 7, 14] is not compatible with the utilization of the PLC devices commonly used in marble machines controlling systems, above all if such techniques must be applied in several points inside the machine.

To address some of the issues of the state-of-the-art slab detection, in this paper we present the experimental characterization of 4 different RFID systems and of 2 capacitive sensing systems in the detection of the presence of the marble slab outside and/or inside the marble machine. Our work aims at a multipoint sensing scheme being contactless, nearly maintenance-free, operating in real-time, robust to harsh environment conditions. The detection aims at providing the machine controlling system with an on/off information concerning the presence of the marble slab under the working tools and is not intended to provide low-scale information on the properties of the material-like composition, thickness, unhomogeneousness due to small cracks, and so forth.

The target of the work, concerning the RFID and capacitive wireless sensing technologies, is highlighting the advantages and the limits of them when applied to detection tasks, mainly in the marble industry process control, and suggesting which technologies are most suitable and how they can be used.

3. RFID for Process Control in Marble Machines

RFID is a mean of identifying, but also tracking and detecting, an item using radio frequency communication, which takes place between a transmitter, usually called "reader," and a transponder (silicon chip connected to an antenna), usually called "tag." The physical coupling is based on magnetic or electromagnetic fields. Tags can either be passive, that is, powered by the reader field, semipassive or active, that is,



(a) (b)

Figure 3: Mechanical sensors and optical sensors at the machine entrance stage.

powered by a battery; in this last case the transmitter is usually the tag itself [16].

At the state-of-the-art the application of RFID technologies has been analyzed and implemented for logistics (for which commercial solutions are available, as an example in the marble industry [17, 18] using 13.56 MHz passive tags and handheld RFID reader), for the management of production [19, 20], and even for localization [21], but less for industrial machine process control and sensing.

In marble machines, the effects on reader-tag communication depend on various parameters: the composition and shape of the stone slab, the operating frequency and power levels of the RFID system, the radiation pattern of the antennas, the distance between tag and reader and their relative orientation, and the working environment (presence of water or dust or a mixture of both, presence of metallic planes in the machine, and composition of the conveyer belt). Hence an experimental test campaign on real case studies using different RFID systems is required. Such experimental campaign, missing in the literature, is the main objective of the present part of the work on RFID technologies.

Since marble machines are not produced in large numbers, therefore not justifying the development of ASICs, in our experiments we implemented 4 RFID systems starting from commercially available tags and readers and customizing the hardware components and/or the relevant software for proper configuration of the experimental setup and for acquisition and processing of test results. Due to the poor availability of experimental data in the literature, we have investigated the application of RFID systems ranging from the low frequencies (LF) to the ultrahigh frequencies (UHF) bands. The four considered RFID systems are shown in Figure 4. The low-frequency RFID system of Figure 4(a) [22] uses passive tags and a communication frequency of 125 kHz; the high-frequency (HF) system of Figure 4(c) at 13.56 MHz uses passive tags [23]; two ultrahigh-frequency systems, at 868 MHz [24], see Figure 4(b), and at 2.45 GHz [25], see Figure 4(d), use, respectively, passive tags and active tags.

The following experiments and related hardware and/or software customizations of the systems in Figure 4 have been realized: (i) measurement and comparison with a given threshold of the amplitude of the signal modulated by the tag and decoded by the reader; (ii) proper setting, through the control software, of the power radiated by the reader antenna; (iii) detection and comparison with a given threshold of the packet reception error rate in the tag-reader communication.

The above solutions are alternatives of each other, and the most suited depends on the possibility of configuration offered by RFID components. As an example in the considered systems [24, 25] the reader power level may be configured. The software of [25] allows processing of communication data to determine the packet error rate. For the test campaign sixteen stone samples, different in size and shape (typically rectangular with the larger sizes in the order of some tens of cm and height of up to a few cm) and representative of the possible materials processed in marble industry (e.g., onyx, marble, granite, etc.), have been considered. In Figure 5 six of the sixteen stone samples are shown.

4. Experimental Analysis of the LF RFID System

The 125 kHz LF RFID system has been firstly characterized in a test setup reproducing the environment inside the marble machine; as sketched in Figure 6 the passive tags have been embedded in fixed positions in the conveyer belt which is made of plastic/rubber and is transparent to LF (the scheme in Figure 6 realizes a smart conveyer belt) or placed under it. The aim of the first test has been the determination of the maximum distances in the 3D space where the tags are detected by the reader without the interposition of the stone samples. In this test the observed output is the data output of the RFID LF reader, see Figure 7, sent to a PC connected to the reader and shown by means of an application providing on/off detection information (plus the code of the tag in case of detection). The LF reader, using a coil antenna with a diameter of about 20 cm (see Figure 4(a)), communicates with passive tags of size 8 cm × 5 cm through inductive coupling. The output power of the reader is 100 mW. Figure 7 also shows the schematic waveform of the signal on the reader coil, highlighting the carrier and its modulation (communication data).

The experimental results, reported in Figure 8, show that the tags can be detected up to a distance of roughly 20 cm in the 3D space. The experiment has been repeated with all

(a) LF 125 kHz (b) UHF 868 MHz (c) HF 13.56 MHz (d) UHF 2.45 GHz

Figure 4: Considered RFID systems (reader, antenna, and tag).

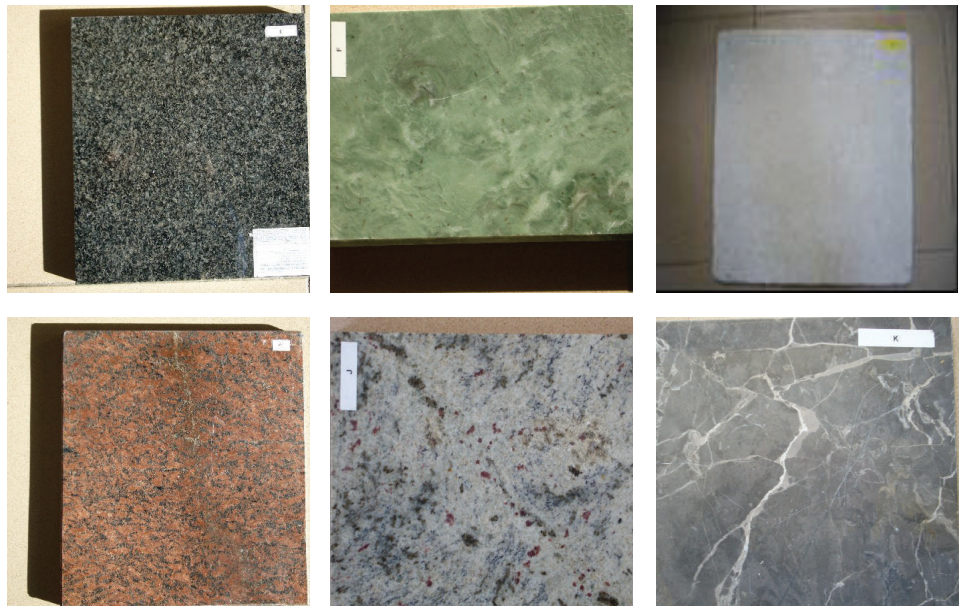


Figure 5: Six of the 16 marble slabs used for the test campaign.

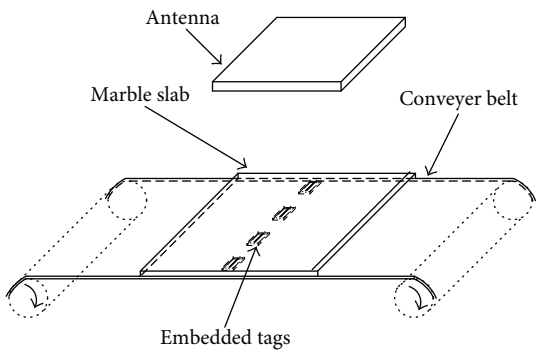


Figure 6: Test configuration with tags embedded in the conveyer belt.

the different stone samples interposed between the tags and the reader coil antenna, with and without the presence of a water layer of some cm and with and without the presence of marble dust and mud. The obtained results are substantially the same of those reported in Figure 8, in which only results on the ZY plane are reported, due to the circular symmetry of the antenna lying on the XY plane.

Experimental results prove that, as expected at the test frequency, stones, water, and mud are almost transparent to LF radiations. Finally we repeated all the above tests analyzing the analog decoded signal in the LF reader, see Figure 7, considering a fixed distance of 10 cm (compliant with the use of the system inside the machine) between the nearest tag and the reader coil antenna. The analyzed signal is obtained through a custom circuit that we added to the reader circuitry in order to filter and measure the amplitude of the decoded signal (envelope of the received signal). Results of these tests are showed in Figure 9. Each reported measurement is generated by averaging ten measurements of the peak-to-peak signal amplitude, with and without interposition of the stone slab between the tag and the reader. The peak-to-peak voltage level measured in absence of stone samples resulted to be 120 mV. Repeating the tests with the stones interposed (more

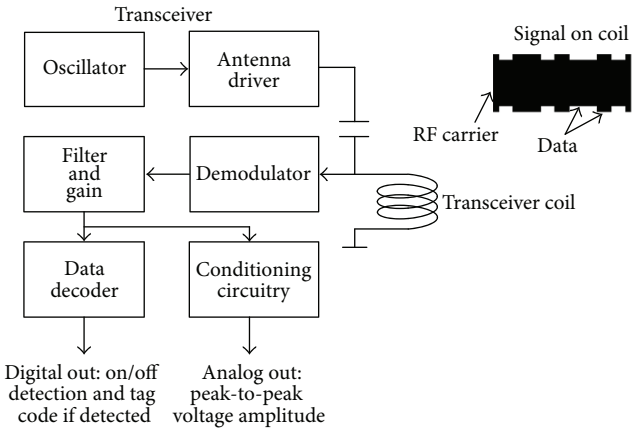


Figure 7: Architecture of the reader, LF RFID system, and schematic illustration of data modulation.

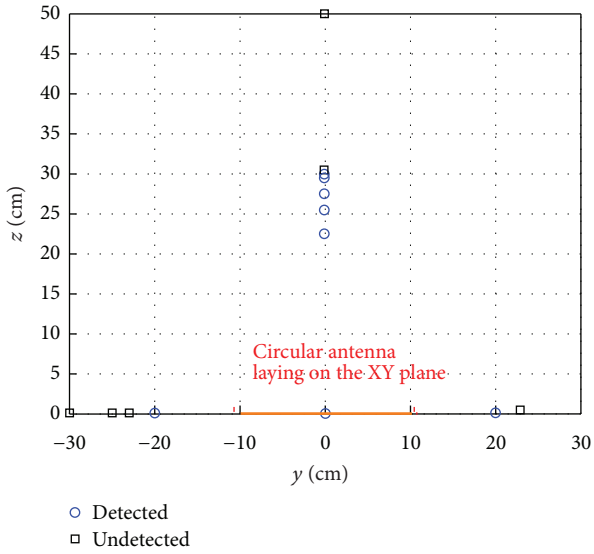


Figure 8: Experimental points of detection, LF RFID system.

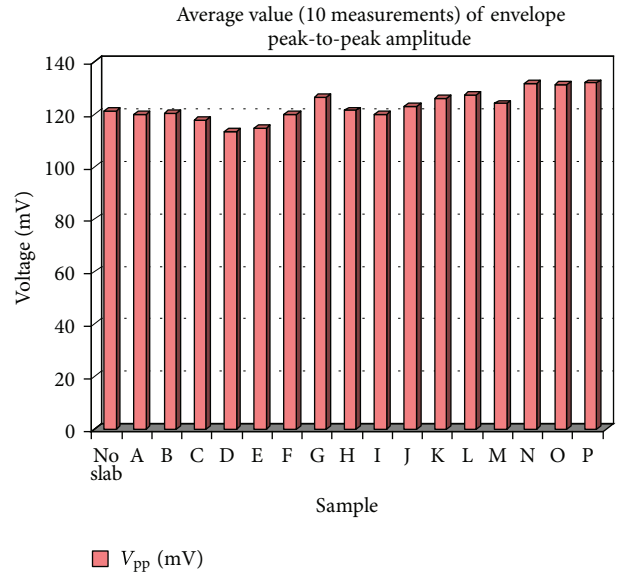


Figure 9: Peak-to-peak amplitude of the decoded signal picked up on the reader by a custom circuitry.

than 16 different stone samples labeled with letters from A to P in Figure 9, with/without water or mud or marble dust), the revealed signal ranged between 115 mV and 125 mV with small differences (within ±4%) versus the 120 mV reference (see Figure 9). Since the measured value slightly depends on the specific type of stone the above detecting technique could possibly be used for industrial applications involving a specific stone type but not in a machinery where the type of stone samples varies from slab to slab.

To solve this issue for the LF RFID system a different detecting strategy has been adopted: instead of embedding the tags in the conveyer belt as in Figure 6, the tag has been applied on the side surface of each marble slab through a fast dry resin as in [17]. The tag is not placed on the top surface of the marble slab in order to avoid any damage by the polishing abrasive heads. The tag has in this case the function of confirming the presence of the slab on the conveyer belt in the position expected by the PLC. This configuration allows the detection, even in presence of water and dirt, of the tag and of the corresponding marble slab when the tag is passing in the area covered by the reader antenna. For the considered LF system the antenna-tag distance should be within 15 cm. Such distance allows the application both outside and inside the machine.

5. Experimental Analysis of the HF RFID System

For the RFID HF system in Figure 4(c), communicating through magnetic coupling with passive tags at 13.56 MHz, by means of a Windows CE application on the handheld device we implemented similar tests and obtained similar results as in the case of the RFID LF system. Figure 10 shows the experimental results concerning the detection limit points in the 3D space without any stone sample interposition. The only difference with the LF system is that the HF system is based on a handheld battery-powered device [23] with an internal tag reader and an internal antenna. Due to the limited radiated power, in the range of tens of mW (typical of HF RFID readers for handheld applications [26, 27]), the maximum reachable distance is below 8 cm. Using an HF RFID reader, not battery powered, a higher power level could be irradiated and hence we expect the achievement of performances similar to those of the LF system concerning the maximum distance of tag reading. As an example, the RFID HF reader [28] technical specifications report a maximum output power of about 4 W and a tag reading distance above 80 cm.

6. Experimental Analysis of the UHF RFID System

For the RFID UHF system, shown in Figure 4(b) and working at 868 MHz, we have firstly repeated the characterization with the test setup in Figure 6 reproducing the marble machine

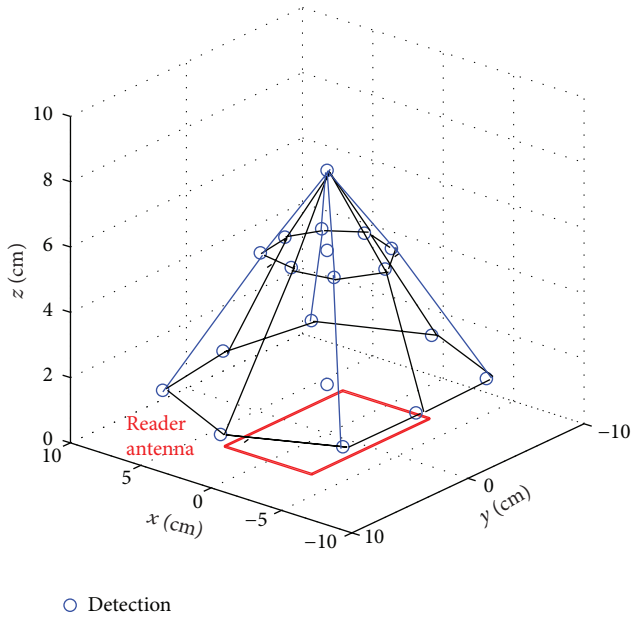


Figure 10: Experimental surface of maximum detection distance, HF RFID system.

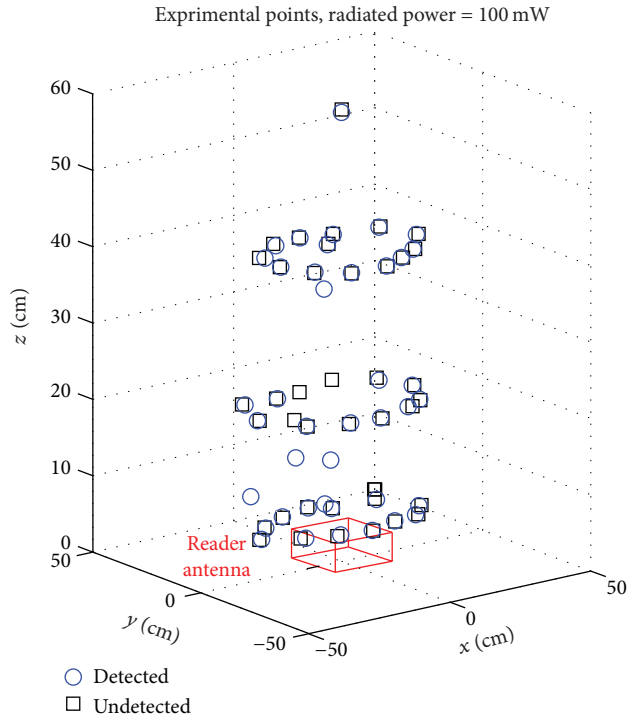


Figure 11: Experimental points of detection, UHF RFID system, for a radiated power of 100 mW.

working environment, embedding the passive tags in fixed positions in or below the conveyer belt. The aim of the first test was the determination of the maximum distances in the 3D space at which the tags are detected by the UHF reader for a defined tag-antenna relative orientation, without interposition of stone samples, at different radiated power levels. Experimental results are reported in Figure 11 for the case example of the reader radiating a 100 mW power. At UHF frequencies the coupling between RFID reader and tags is electromagnetic.

The power level irradiated by the UHF reader antenna is programmable in the range [100 mW, 4 W]. To be noted is that power regulations in Europe are characterized by a limit of 500 mW while the maximum level of 4 W is permitted by US regulations.

Besides the irradiated power level also the working frequency of the selected UHF reader [24] is programmable in order to support both European and US regulations. The used tags are passive devices compliant with the ISO18000-6B standard and compliant with both US and European regulations concerning frequency and power levels. The antenna is a planar one with a wide frequency working range from roughly 800 MHz to 960 MHz. To carry out the test campaign, the Microsoft Visual C++ PC application controlling the UHF reader has been modified and customized in order to provide an interface suitable for testing purposes. In Figure 12 the customized graphical user interface (GUI) is shown. Figure 13 reports the maximum distance at which the tag is still detected as a function of the reader antenna power level.

The experiment has been repeated with all the different stone samples interposed between the tags and the reader antenna, with and without the presence of a water level of few cm and with and without the presence of marble dust

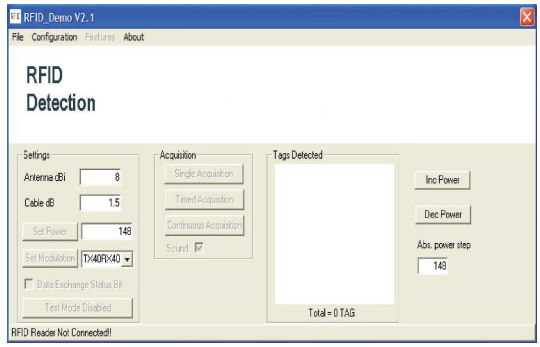


Figure 12: The customized GUI of the application for the UHF reader control.

and mud. Differently from what measured in the case of LF and HF systems, at UHF frequencies the communication is completely shielded by water, that is, in presence of a thin layer of water, or in some cases just with a few water drops wetting the tag, the tags are not detected. These experimental results are aligned with studies [29] on water properties, see Figure 14, proving that in the UHF range the intensity of a plane incident wave decreases to $1/e$ (i.e., 63% absorbed) in a penetration distance of about 1 cm or lower depending on the test conditions (note that in our application the water layer can be of some cm). Therefore UHF systems cannot be used inside the marble machine.

The results of the test campaign applied using the configuration of Figure 6 with different types of stones interposed (in a dry environment) prove that at UHF frequencies a stone

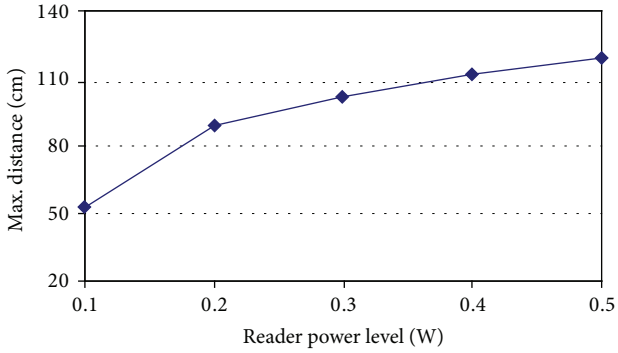


Figure 13: Max. distance of tag detection versus radiated power.

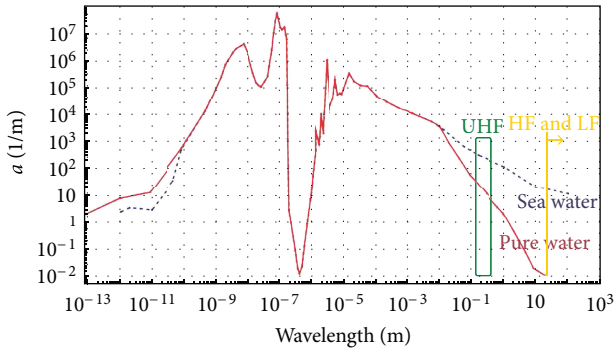


Figure 14: Water absorption spectrum.

sample attenuates the RF signal. Therefore the tags embedded in the conveyer belt can be detected or not depending on the distance and power level radiated by the reader.

According to this result the detection of the marble slab with UHF systems is possible following the strategy described hereafter. First, as sketched in Figure 6, the tags should be embedded in the conveyer belt while the reader antenna should be attached on the upper part of the machinery in a fixed position (e.g., 40 cm above the conveyer belt in our case study). Secondly, the emitted power level should be properly configured so that (a) when the stone sample is interposed between the tag and the reader antenna the RF signal is attenuated under a certain bound and the tag cannot be detected by the reader; (b) when the stone sample is not present the tag communicates correctly with the reader. After the test campaign in a dry environment we determined that configuring the UHF reader with a radiated power ranging from about 400 mW to 600 mW the detection of stone samples is allowed according to the above on/off strategy. The experimental results of this test are reported in Figure 15 for a case study of slabs sized about 30 cm × 30 cm. Hence configuring the reader with a proper power level in this range (e.g., 500 mW) and embedding the tags in the belt, a RFID UHF system can be used for automatic detection in the process control of marble industry. It must be pointed out that this type of detection is possible only in a dry environment; therefore it cannot be used inside the machine where a water layer of several millimeters is always present.

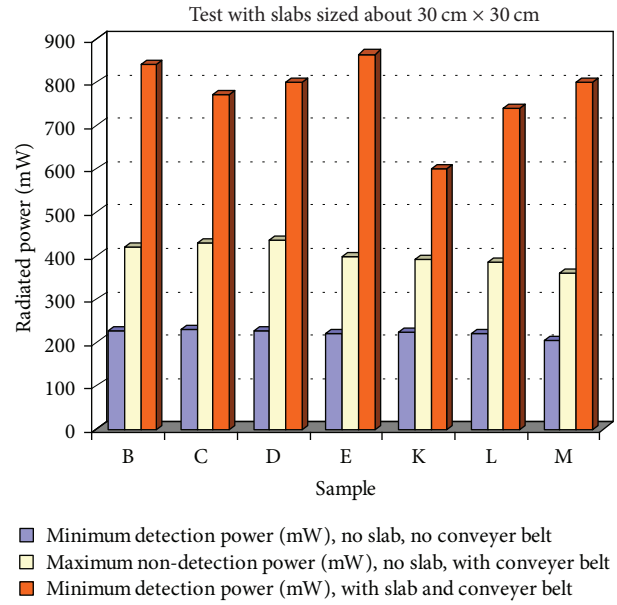


Figure 15: Experimental results showing the radiated power in the on/off detection strategy test.

On the contrary, outside the machine, in a dry environment, the UHF RFID system represents an interesting alternative to traditional mechanical and optical systems to detect the presence of the marble slab at the entrance of the machine. With respect to mechanical sensors, the UHF RFID systems benefit of being contactless. With respect to optical systems the UHF RFID solution is more robust to the presence of a dirty environment.

7. Experimental Analysis of the Microwave Active RFID System

For the RFID UHF system at 2.45 GHz we implemented tests similar to those carried out for the RFID system at 868 MHz. One of the main differences is represented by the fact that the 2.45 GHz solution, shown in Figure 4(d), uses active tags and its maximum detection distance, without the marble slab, is up to 20 m at 1 mW of effective radiated power. Since the distance to be covered in marble machine applications is below 50 cm, during the tests we configured the 2.45 GHz RFID tags for 1/16 mW effective radiated power in order to limit the operating range at a few tens of cm when the marble slab is not present. For the 2.45 GHz active system, the slab detection strategy is not based on the reception/no reception of data packets transmitted by the active tag but on the measure of the reception error ratio and its change in the two cases of slab interposed and not interposed between the tag and the receiver antenna. Reception errors are due to RF absorption and/or scattering by the stone. In the following, the reception ratio refers to the number of correctly received packets divided by the number of expected (i.e., transmitted) packets. For the considered 2.45 GHz RFID system, a data packet is transmitted every about 250 ms (4 packets per second); transmission power is cyclically changed every data

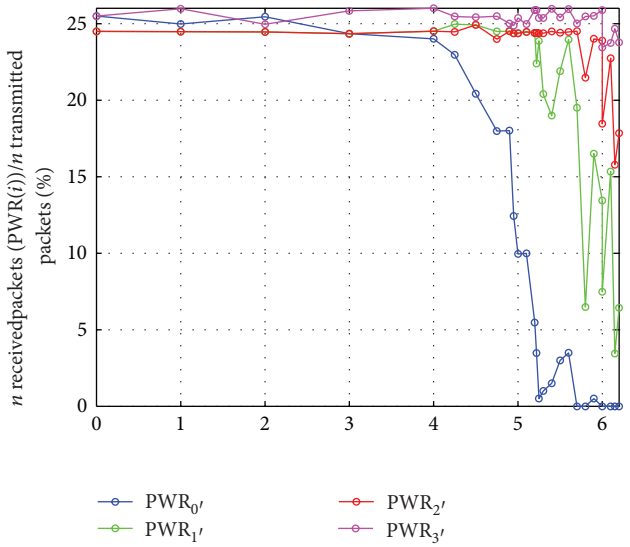


Figure 16: Reception ratio versus tag-reader distance for the ith emitted power level (1/64 mW, 1/16 mW, 1/4 mW, and 1 mW, resp., PWR_0, PWR_1, PWR_2, and PWR_3).

packet in the set of 4 different radiated power levels: 1/64 mW, 1/16 mW, 1/4 mW, and 1 mW. Obviously the reception error rate can be calculated as 1 minus the reception rate of correct data packets.

In order to collect experimental data, we developed an ad hoc Matlab (from the Mathworks) application on a PC processing data received by a USB 2.45 GHz receiver. Packets received with errors are discarded and therefore counted as nonreceived. The original firmware (C) on the tag and on the receiver was customized in order to format data packets according to data processing needs.

Preliminary tests were carried out in order to confirm that with transmitter and receiver placed at a short distance the reception rate was 100% for each power level, therefore excluding buffer overflow problems on the receiving PC (e.g., due to application overhead problems). To be noticed is that the packet distribution is not exactly 25.0% for each power level, but about 25.5%, 24.25%, 24.5%, and 25.75% for packets at 1/64 mW, 1/16 mW, 1/4 mW, and 1 mW power, respectively, as measured in several experiments and in conditions of no packet loss. Figure 16 shows the reception ratio in percentage for each power level as a function of the tag-reader distance, measured in a first experiment carried out in a mixed indoor/outdoor environment.

For the power of 1/64 mW, Figure 16 shows a monotonic decrease and a knee in the curve of reception ratio versus distance. Curves at different power levels have not exactly the same trend of the curve for the power of 1/64 mW, probably due to reflections and/or other scattering effects in the working environment, that should of course be characterized and/or avoided in on-field applications.

To achieve the best sensitivity in the reception ratio, the experimental setup for slab detection was arranged by properly displacing tag and receiver antenna so that the reception ratio without the slab was below 100%, ideally on a working point in the decreasing part of the curve after the knee, in order to have a good sensitivity of the reception ratio versus slab interposition.

Table 1: Relative dielectric permittivity of different materials.

Material	Dielectric permittivity, ε_r
Bianco Carrara	5.7
Rosa Portogallo	6.8
Pietra di Trani	13.8
Granito Grigio	29.9
Pietra del Cardoso	9.2
Ceramics	4.3–6.7
Plastic (PVC, Plexiglass)	2-3

During tests with the sixteen slabs we carried out about five measurements of the error ratio just a few seconds before any slab interposition in order to avoid drifts due to possible environmental effects and then during slab interposition. The two sets of measured values are reported in Figure 17, linked by a line identifying the progression of the experiment. With this configuration, when the marble slab is not passing, the reception ratio is from 40% to 80% while with slab interposition, in most cases, the reception ratio drops below 10%–20% (i.e., the reception error rate is up to 80%–90%); this decrease is interpreted as detection of the stone sample, but in some cases (slab B, E, J, L) the presence of the slab causes an increase of the detection ratio instead of a decrease. Since the behavior of the system depends on the specific type of stone, the described detecting technique could possibly be used only for applications involving a specific stone type but not in a machine where the type of stone sample is not known a priori.

To be noted is that the considered 2.45 GHz RFID system has two main disadvantages:

(i) its use is possible only at the entrance of the marble machine in a dry environment since, as in case of the 868 MHz RFID system of Section 6, also microwave signals are absorbed by water;

(ii) the use of active tags causes a higher cost for the tags. Therefore the solution with passive tags should be preferred for process control applications in the marble industry.

8. Capacitive Sensing Principle and Front-End Circuitry for Marble Detection

To address some issues of the currently used and of other proposed slab detection techniques, this section of the work proposes novel capacitive sensors for the detection of stone samples during the industrial process, inside and outside the machine, and by means of contactless and low-complexity devices. Indeed, as reported in Table 1, the stone samples used in the marble industry have relative dielectric permittivity ε_r in the range 5 to 30 [5, 9, 10] that can be used to reveal the presence of a stone sample being different from those of air ($\varepsilon_r = 1$), water ($\varepsilon_r = 81$), or plastic (ε_r between 2 and 3).

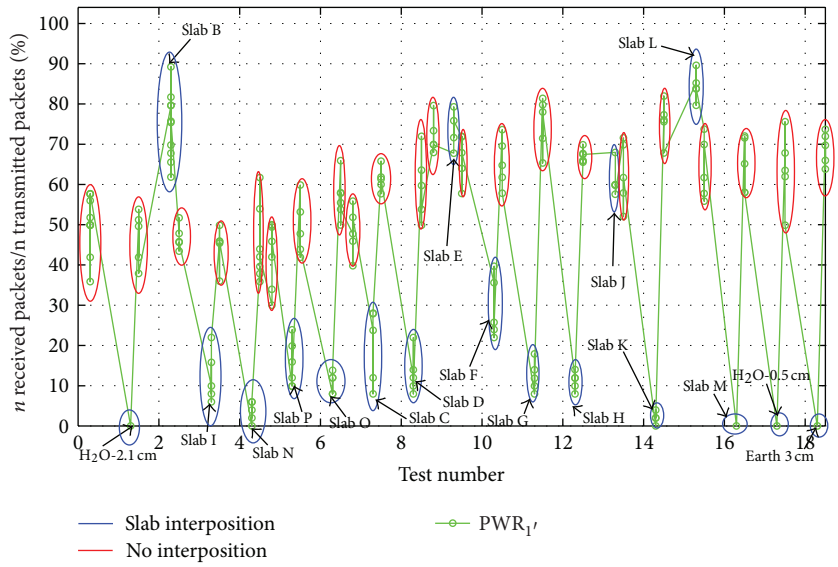


FIGURE 17: Reception ratio normalized to 100% measured with/without slab interposition for radiated power of 1/16 mW.

As mentioned in Section 2, capacitive sensors have been studied in the literature [9] but the solutions proposed are optimized for a fine-grain analysis of the porosity and surface defects of the stone material in a controlled working environment (dry and clean) rather than the real-time detection of a marble slab in an industrial machine. Furthermore in [9] the realized sensor should be taken in contact with the stone sample with a controlled force of 1 N and the stone sample should be held in a fixed position. Instead the aim of our work is the contactless detection of the presence of stone samples moving on the conveyer belt and considering a real industrial environment characterized by the presence of mud, water, and stone residuals and is not intended to measure or give information about material properties (e.g., thickness, composition, unhomogeneousness, etc.).

The basic scheme exploited in this work is the capacitor with parallel metallic plates filled with multiple layers of different dielectric materials; see Figure 18 for the schematic representation in case of a number of dielectric layers $n = 3$.

The value of the capacitance can be determined considering the series of n capacitors each of value $C_i = \varepsilon_o \cdot \varepsilon_{ri} \cdot S/d_i$ with $i = 1, \ldots n$, being S the area of the metallic plates, and d_i and ε_{ri} the thickness and the relative dielectric permittivity of each layer.

Firstly we realized a capacitive sensor with plates sized 6.5 cm × 12.5 cm (S roughly 80 cm^2) in a test-bed reproducing a marble machine working environment found at the machine entrance stage, without the presence of water (note that the characterization of the sensing system with a test-bed considering the presence of water will be discussed in Sections 9.1 and 9.2). The total distance D between the plates has been fixed at 4.5 cm to allow the contactless interposition of different stone samples which have a typical thickness between 1 and 3 cm. The reported analysis is still valid for case studies with maximum thickness higher than 3 cm by increasing, accordingly, the distance D between the plates. Mounted at the entrance of the marble machine, the capacitance value, when the marble sample is not present, is expressed by (1) and amounts to about 1.6 pF:

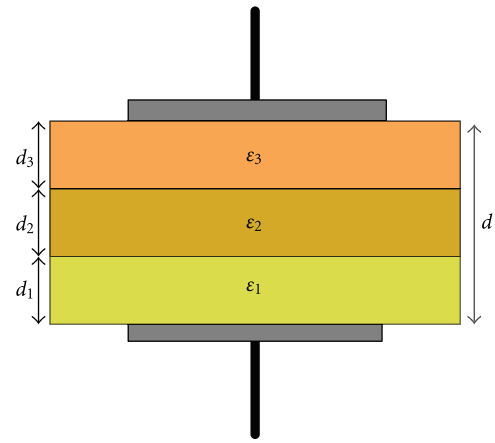


FIGURE 18: Multidielectric layer capacitive sensor.

$$C_0 = \varepsilon_o \cdot \frac{S}{D}. \tag{1}$$

In this case the filling dielectric is just air. When a stone sample of relative dielectric permittivity ε_r and thickness x is passing through the metallic plates, see Figure 19, the capacitor value C_{sens} is expressed by (2), and the ratio C_{sens}/C_0 is expressed by (3):

$$C_{\text{sens}} = \varepsilon_o \cdot \varepsilon_r \cdot \frac{S}{[x + \varepsilon_r (D - x)]}, \tag{2}$$

$$\begin{aligned} \frac{C_{\text{sens}}}{C_0} &= \varepsilon_r \cdot \frac{D}{[x + \varepsilon_r \cdot (D - x)]} \\ &= \frac{\varepsilon_r}{[x/D + \varepsilon_r \cdot (1 - x/D)]}. \end{aligned} \tag{3}$$

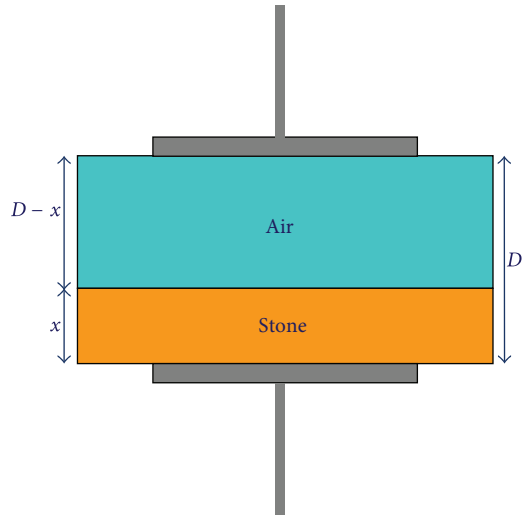


Figure 19: Multidielectric layer (air/stone) capacitive sensor.

For typical stone samples ε_r ranges from 5 to 30, see Table 1, and x/D ranges from 0.25 to 0.75 for the selected value $D = 4.5$ cm. Therefore, when a stone sample is passing, the capacitor value is increased with a ratio C_{sens}/C_0 expressed by (3). As a consequence, the detection of the stone sample can be simply realized by revealing a change in the capacitor value higher than a given threshold. The easiest way [30, 31] to reveal this change is inserting the capacitive sensor in an astable circuit and measuring the shift of the oscillating frequency with a microcontroller-based circuit, as shown in Figure 20. The astable circuit is realized with a simple 555 IC and has a theoretical oscillating frequency expressed by

$$F = \frac{1}{\left[\ln(2) \cdot (R_A + 2R_B) \cdot \left(C_{\text{sens}} + C_p + C_{\text{ext}}\right)\right]}. \quad (4)$$

In (4) C_{sens} refers to the capacitive sensor, C_p to the open-circuit parasitic capacitor due to wire connections and astable component input capacity, and C_{ext} to an external capacitor inserted to set at a desired value F_0 the oscillation frequency when $C_{\text{sens}} = C_0$. This way the capacitance change is transformed in a frequency change, easily revealed through a low-cost low-power [32] 8-bit microcontroller.

With marble interposition the value of C_{sens} in (2) increases and hence the oscillation frequency in (4) decreases. To be noticed is that the size of the surface plates S does not influence the change of the capacitance ratio $C_{\text{sens}} = C_0$; the value of S is important to determine absolute values of C_{sens} and C_0 giving measurable variation in (4).

After realizing the circuit we implemented a test campaign using 16 stone samples, different in size and shapes (typically rectangular with horizontal size in the order of several tens of cm and height of up to a few cm), representative of the possible materials processed in marble industry (e.g., onyx, marble, and granite). Snapshots of 6 of the 16 different stone samples used during the testing campaign are reported in Figure 5.

The obtained results are summarized in Figure 21 which reports the frequency change with respect to F_0 for each stone sample (labeled with a letter in the range [A,…,P]). The frequency changes in Figure 21 range from a minimum of 2.6 kHz (sample K in Figure 21) to a maximum of 26 kHz (sample I in Figure 21) allowing a reliable detection of the stone presence. The astable circuit reference frequency is set at $F_0 = 219$ kHz, see in Figure 22 the snapshot of the signal generated by the circuit in Figure 20 when $C_{\text{sens}} = C_0$. The tests have been carried out also in the presence of mud, marble dust, and powder, obtaining results similar to those in Figure 21.

In the test campaign, we used a threshold for frequency change detection of 1 kHz which ensures a margin of 1 kHz against false detections and higher than 1.6 kHz (the minimum 2.6 kHz decrease when a stone is present minus 1 kHz threshold) against missed detections. Since our goal is an on/off detection, the above margins are sufficient to avoid errors caused by changes in the reference frequency during the time occurring for a typical slab to pass under the sensor (up to tens of seconds); such reference frequency changes can be caused by parasitic capacitance change, deposition of marble dust or mud, and change of temperature conditions. To face slow variations of the reference frequency, the microcontroller via software can monitor F_0 and manage adaptive thresholds.

It is worth noting that in our proposed front-end circuitry the capacitance change (due to the stone slab presence) is detected through a frequency change with respect to the fixed frequency value F_0. To further increase the robustness of our system to electromagnetic interference (EMI), typical of industrial environments, a variable resistor R_B can be used in the scheme of Figure 20 to tune the value of F_0 according to (4). This way when applying the proposed sensing system in a specific industrial environment during the system calibration phase the frequency F_0 can be set in a range where the EMI is null or minimal by changing the value of R_B. To this aim Figure 23 shows that to change F_0 in the range [100 kHz–500 kHz] it is enough to change R_B in the range [5 kΩ–100 kΩ]. These values have been sized under the hypothesis, which is always verified in our experimental tests and in industrial systems we considered, that in the selected range [100 kHz–500 kHz] there is at least a pass-band channel of several kHz where the level of EMI does not interfere with the signals in the circuitry of Figure 20.

The change of R_B can be implemented directly by the microcontroller in Figure 20 by using a digital-controlled potentiometer. The control of R_B has been preferred to the control of R_A since in (4) R_B has a weight double of the one of R_A.

9. Capacitive Detection

9.1. Multidielectric Capacitive Sensing for Marble Industry. Once demonstrated in Section 8 the effectiveness of the sensing and reading principle some modifications have been applied to the schemes in Figures 18, 19, and 20 for a successful integration in a real marble machine. Indeed, as discussed in Section 2 and illustrated in Figure 24, in a marble machine the stone samples are placed on a plastic belt with a thickness B less than 1 cm (0.5 cm typical) sliding

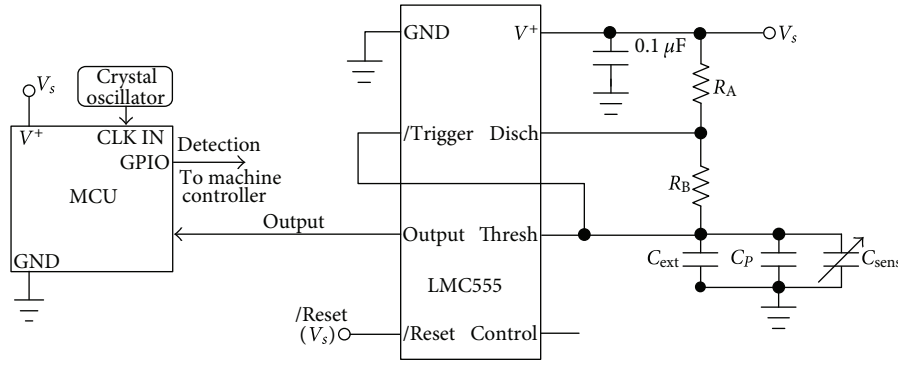


Figure 20: Front-end circuitry for capacitance change detection.

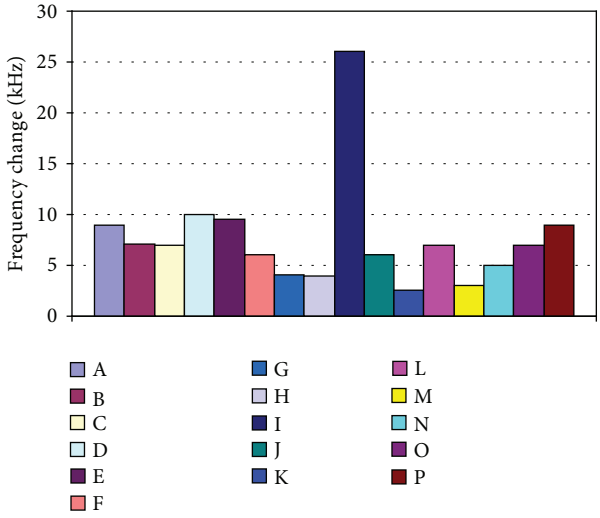


Figure 21: Frequency change for different stone samples, 2-plate capacitor.

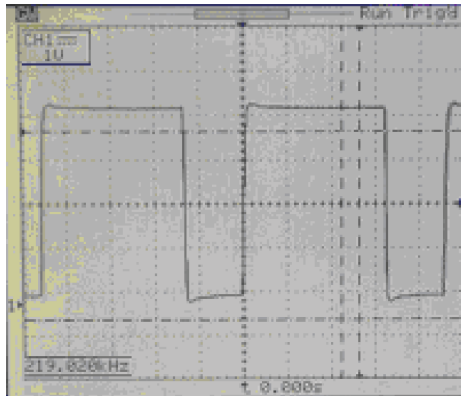


Figure 22: Snapshot of the astable output signal at F_0.

on a metallic plane. Hence the capacitive sensor can be simply realized suspending a conductive plate (top plate of the capacitor) over the already existing metallic plane of the industrial machine (bottom plate of the capacitor) at a distance D. Since the metallic plane surface is larger than

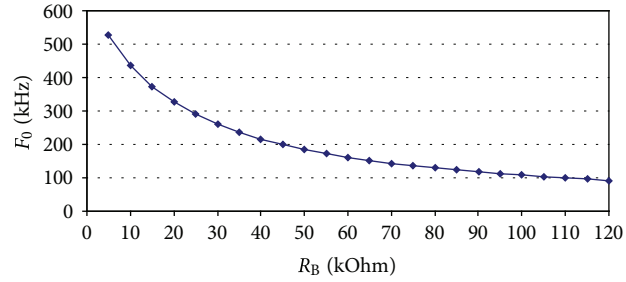


Figure 23: Change in F_0 versus change in R_B for the circuit in Figure 20.

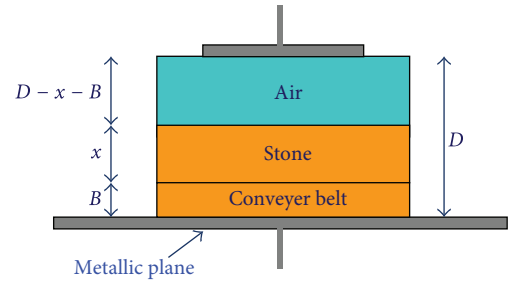


Figure 24: Multidielectric layer (air/stone/plastic belt) capacitive sensor inside the marble machine.

the metallic plate one, the method of image charges [33] can be applied: the new capacitor is equivalent to that of Section 8, (1) to (3), but with an effective distance $2D$. With respect to the analysis in Section 8 we have also to consider that in absence of the stone sample the filling dielectric is made up of a layer of $B = 0.5$ cm of plastic material (with ε_{rb} between 2 and 3) and a layer of air of thickness $D - B$. The reference capacitance C_0 is now determined by

$$C_0^{-1} = \left[\varepsilon_o \cdot \frac{S}{2(D-B)}\right]^{-1} + \left[\varepsilon_{rb}\varepsilon_o \frac{S}{2B}\right]^{-1}. \quad (5)$$

Considering $D = 4.5$ cm and $S = 80\,\text{cm}^2$, C_0 in (5) amounts to roughly 1 pF. When a stone sample of constant ε_{rx} and thickness x is passing through the metallic plates, a change in the capacitance value occurs since the capacitor is

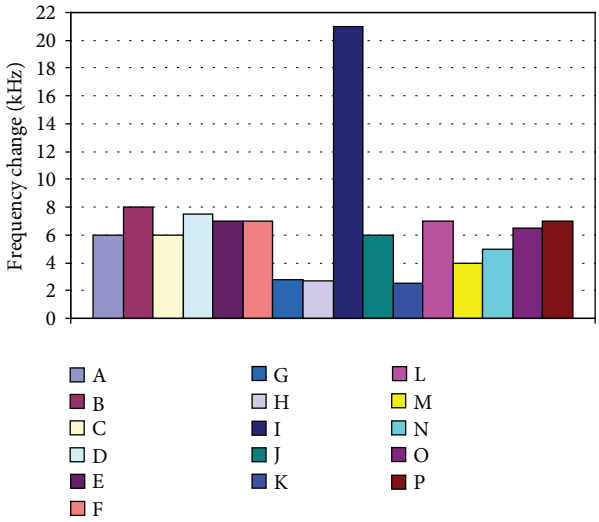


Figure 25: Frequency change for different stone samples, 1 plate capacitor.

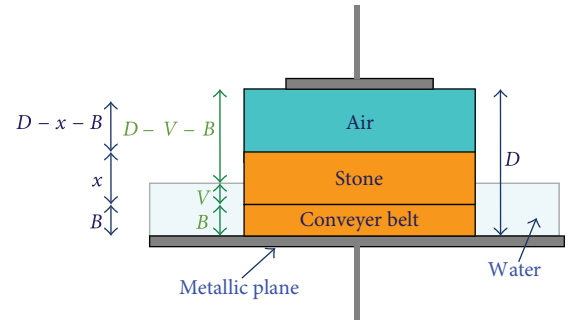


Figure 26: Multidielectric layer (air/stone/plastic belt) capacitive sensor inside the marble machine with water.

filled by three dielectric layers: a layer of $B = 0.5$ cm due to the plastic belt, a layer of x cm due to the stone, and a layer of air of size $D-x-B$. As a result of the stone interposition there will be a change of the capacitance C_{sens} (the value increases) that can be read as a frequency change in the circuit of Figure 20 (the oscillation frequency decreases with respect to the reference value F_0 obtained when $C_{sens} = C_0$).

Implementing a test campaign with the new designed sensing circuit using the 16 stone samples mentioned in Section 3, different in size and shapes, and representative of the possible materials processed in marble industry (e.g., onyx, marble, granite,…etc.) the results of Figure 25 are obtained: the frequency change ranges from a minimum of 2.5 kHz (K sample in Figure 25) to a maximum of 21 kHz (I sample in Figure 25) allowing a reliable detection of the stone samples.

The tests have been implemented also in presence of mud, marble dust, and powder obtaining similar results. As discussed in Section 8, since our goal is an on/off detection, a frequency change threshold of about 1 kHz allows for sufficient margins against false or missing detections due to parasitic capacitance change, deposition of marble dust or mud, and changing of temperature conditions during the typical measure time (1 second and up to tens of seconds). Reference frequency variations in a larger time scale can be managed through the microcontrollers via software by monitoring F_0 and adapting the thresholds accordingly.

The correct behavior of the capacitive detection system with capacitive to frequency conversion has been confirmed also considering the presence of water inside the machinery.

In this case, see Figure 26, when the stone sample is not passing the reference capacitor value C_0 can be calculated considering a layer of size B of roughly 0.5 cm due to the plastic belt in series with a layer of size V (few cm) filled by water and a layer of size $D - (V + B)$ filled by air. When the marble stone is interposed between the metallic plates it removes the water and the new capacitor value C_{sens} can be calculated considering a layer of size B for the conveyer belt in series with a layer of size x and dielectric constant ε_{rx} and a layer of size $D-(x+B)$ filled by air. By detecting the capacitor change through a frequency change reusing the astable circuit (see Figure 20) the presence of a stone sample can be revealed in a reliable way. Repeating the test campaign using the 16 stone samples, different in size and shape, and in presence of water the frequency change is at minimum 1.5 kHz.

Summarizing, the proposed scheme can be easily implemented in a real marble machine, it is a low-complexity scheme with low maintenance cost, it is contactless, and it allows the reliable detection of stone samples also in presence of water, mud, and marble dust with enough margins against miss detections or false hits. The detection signal generated by the microcontroller may be sent to the main PLC controlling the working heads (see Figure 20). Though presenting a lower value of C_0 for a given surface S of the plate, the single-plate capacitor solution has the great advantage versus the 2-plate capacitor discussed in Section 8 of not requiring the positioning of the second metallic plate under the conveyer belt, since the already existing metallic plane of the industrial machine is used. This way cabling and system maintenance are simplified.

9.2. Surface Capacitive Sensing for Marble Industry. In this section we propose a new capacitive sensor configuration, derived as an adaptation of the theory developed by Bozzi and Bramanti in [9]. Then we compare the obtained solution with the one proposed in Section 9.1.

In [9] Bozzi and Bramanti realized a capacitive sensor, see Figure 27, through the use of three copper conductive lines printed over a piece of FR4 dielectric material ($\varepsilon_r \sim= 4.5$) with a thickness T of 10 mm: the central copper line, acting as signal line, is separated by a narrow gap W from the two other lines, joined together at one end and acting as ground lines. The lines are separated by a distance $W = 1$ mm, and therefore $W \ll T$.

As proved in [9] this device is sensitive to the average value of the dielectric permittivity (ε_{r2} in Figure 27), of the material which is present at a distance H from its surface, with $H \leq W$. As an example if the device in Figure 27 is put in contact with a material with dielectric value ε_{r2}, the device has a capacitance expressed by (6) where k is a constant whose

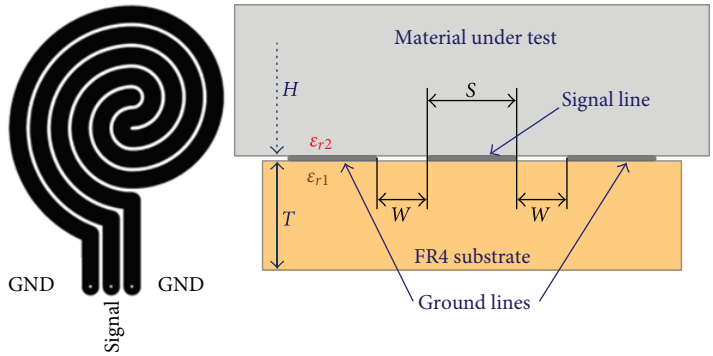


Figure 27: Surface capacitive sensor from [9].

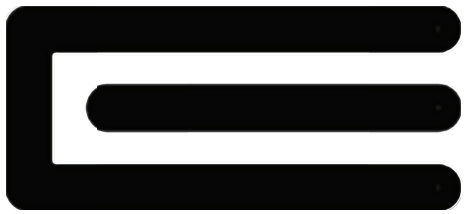


Figure 28: Modified surface capacitive sensor.

size depends on the ratio between the width of the lines, S, and their distance, W.

As suggested in [9] and realized in Figure 27, S should be comparable to W while the total track length L should be much higher than S and W:

$$C = 2\left(\varepsilon_{r\mathrm{FR4}} + \varepsilon_{r2}\right) \cdot \varepsilon_o \cdot k. \tag{6}$$

The above sensor has been used in [9] to reveal, on static samples, the surface value of the dielectric constant of materials by reading through a capacimeter the value of the capacitance between the signal and the ground lines. The sensor devised by Bozzi and Bramanti is a contact sensor for surface analysis: it is sensitive to the material property within a distance H of about 1 mm from its surface.

Starting from the Bozzi and Bramanti theory we modified the sensor in order to

(a) use an FR4 plane with a thickness of 1.6 mm, compliant with standard printed circuit board (PCB) technology and much lower than the 10 mm used in [9]; indeed the size used in [8] is not compliant with standard PCB technologies and hence implies a high device cost in case of industrial production;

(b) change the shape and size, see our new device in Figure 28, of the printed capacitor to be sensitive within a range H of at least 2 cm from the surface.

The condition in the above point (b) is essential to allow a contactless detection of the presence of a stone sample. However, for the device in Figure 28, as in [9], the thickness of the sensitive area H is determined by the distance W between the conductive lines printed over the FR4 substrate. To achieve a thickness H of roughly 2 cm the device in Figure 28 has to be sized with a distance between the lines W of about 2 cm. The width S of the printed conductive lines in Figure 28 is 2.5 cm, while the larger side of the sensor has a size $L = 22$ cm (according to the approach of Bozzi and Bramanti in [9] L should be much higher than W). As a result, to achieve a thickness H of roughly 2 cm a total area of 220 cm^2 is required for the surface capacitive sensor, 2.75 times larger than the area of the capacitive sensors in Sections 8 and 9.1 which is 80 cm^2. This is a bottleneck of the surface capacitive sensor presented in this section when compared to the capacitive sensor in Section 9.1. Indeed scaling all dimensions of Figure 28 to achieve a sensing thickness of 4 cm, as in Section 9.1, the required area will increase up to 1300 cm^2. For this reason the device in Figure 28 has been sized for a value of $H = 2$ cm, a good tradeoff between sensitive thickness and sensor area.

Figure 29 reports the impedance Z_{in}, real and imaginary (absolute value) parts, offered by the sensor in Figure 28 as a function of the frequency, derived from an analysis with the electromagnetic simulator ADS (advanced design system) by Agilent Technologies. For sake of clarity two figures are reported referring to a frequency range from 10 Hz to 1 kHz and a frequency range from 1 kHz to 1 MHz.

The proposed sensor in Figure 28 can be suspended over the conveyer belt at a height of 3 cm (to leave enough space for the stone samples in the considered application case study of a thickness ranging from 1 to 3 cm). When there is not any stone to detect ε_{r2} in (6) is 1 (air) and the sensed capacitive value represents the reference value C_0. When a stone is passing, the device can reveal its presence as a change in the capacitance value that can be converted through the astable circuit of Figure 20 in a frequency change. As already discussed when the stone is detected the capacitance value from (6) is increased and the oscillation frequency from (4) is decreased.

Implementing a test campaign with the sensing circuit designed in Figure 28 using the 16 stone samples, different in size and shape, already adopted in Sections 8 and 9.1, the results of Figure 30 are obtained.

The frequency changes in Figure 30 range from a minimum of 2 kHz to a maximum of 7 kHz allowing a reliable detection of the stone samples.

Table 2: Main performance of the RFID systems (passive tags) for marble slab detection.

RFID System	LF 125 kHz	HF 13.56 MHz	UHF 868 MHz
Radiated power	100 mW	<50 mW	<500 mW
Max. stone detection distance	15 cm	<8 cm	<40 cm
Best tag placement	Side surface of the marble slab		Embedded in the conveyer belt or under it
With water	Works		Does not work
With dust/dirt/stone residuals	Works		

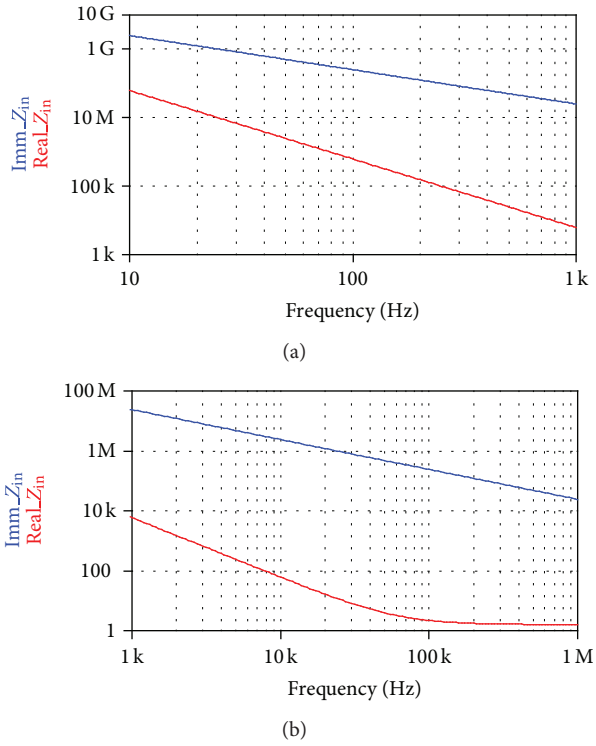


Figure 29: Real and imaginary (absolute value) parts of the surface capacitive sensor in Figure 28 (10 Hz–1 kHz and 1 kHz–1 MHz ranges) versus frequency.

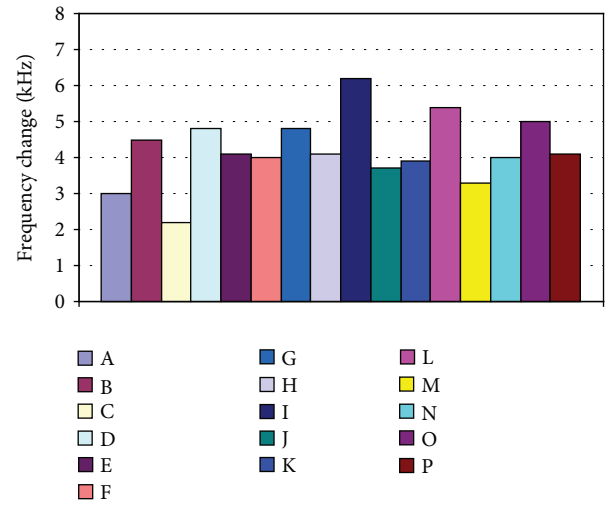


Figure 30: Frequency change versus stone sample, surface capacitor.

Repeating the test in presence of water, marble dust, or mud we obtained similar results.

10. Discussion on the Application of the Analyzed Sensing Technologies

10.1. Comparison among the Different Analyzed Contactless Sensing Solutions. As illustrated in Section 4 to Section 7, the experimental analysis of the 4 RFID technologies has been carried out using a test setup reproducing environmental conditions representative of those found inside the marble machine, with water, mud, marble dust, and considering more than 16 different types of stones. The experimental results are schematically reported in Table 2.

Test results proved the following.

(i) Passive tags have to be preferred to active tags since the marble slab detection can be implemented with lower costs and easier system maintenance (e.g., no battery to be replaced). Table 2 summarizes the main performances of the analyzed RF detection systems using passive tags.

(ii) All types of stones are transparent to the tested 125 kHz LF and 13.56 MHz HF radiations; hence for these RFID systems the most suitable strategy for a reliable detection is applying the tag on the side surface of each marble slab by means of a fast dry resin. This allows the detection, even in presence of water and dirt, of the tag and of the corresponding marble slab when the tag is passing in the area covered by the reader antenna. This strategy is useful anyway to confirm to the heads controlling system the presence of the marble slab in the expected point of the machine. The tag, placed in this position, can be used also to store information for logistic applications and for the traceability of the different industrial processes applied to each slab [17].

(iii) UHF communication at 868 MHz and 2.45 GHz is shielded by water and hence UHF systems can be used just outside the machine (dry environment): with respect to mechanical sensors, the RFID systems benefit of being contactless. With respect to optical systems the RFID ones are more robust to the presence of marble dust and dirt. The detection of the marble slab is possible according to the on/off strategy described in Section 6 by properly configuring the UHF system

and possibly to the detection strategy presented in Section 7 concerning active RFIDs at 2.45 GHz. In the latter case, anyway, the behavior of the RFID system depends on the specific type of stone, and therefore the described detecting technique could be suitable just for applications involving a stone type a priori known.

It is worth noting that the above-described detecting techniques using passive tags require low-cost tags (one for each marble slab or a set embedded in the conveyer belt) and an antenna for each head of the machine or serving a few consecutive heads. Multiple antennas (e.g., up to 4 for the RFID system in [24]) can be controlled by the same reader positioned outside the machinery since the reader and its antenna are typically connected through cables whose length amounts to some meters.

The application of contactless sensing of the presence and/or the position of the marble slab by means of RFID technologies also have a direct benefit on the possibility to avoid or reduce cabling inside or outside the machine for sensor data transmission to the machine controlling system. For passive RFID tags, no cabling among them is needed, while in the case of active RFID tags (usable only outside the machine) supply should be provided to tags (batteries need maintenance, and energy harvesting appears not to be practical or possible at the required transmission rate).

Passive RFID tags implement a wireless sensor network coordinated by the RFID reader.

The possibility offered by RFID technologies of multitag detection and collision management system allows for the implementation of linear sensor (tag) arrays placed under the conveyer belt at the machine entrance stage. For a typical case study, a tag spacing of 10 cm would allow a usable spatial resolution in slab sampling. At this aim, about 30 tags can constitute a tag array covering the conveyer belt width (in the order of 3 m), and, depending on the particular RFID technology used, multitag reading is possible at a rate sufficient to read a tag array every one-two seconds by means of one or more RFID antennas and/or readers. In such a way, slab presence detection and slab shape detection may be realized for process control. The tag IDs are provided as data output by the RFID readers on a serial or Ethernet port. RFID readers may be connected through a point-to-point (or multipoint-to-point) connection to

(i) the PLC, if its processing power is sufficient to command/configure the RFID readers, receive detected tag IDs, and transform them into slab sampling information;

(ii) an intermediate intelligent data collecting and processing device, for example, a microcontroller-based one, able to command/configure the reader and to apply detection algorithms, sending to the PLC only the final detection data.

Concerning the LF and HF RFID systems, tags are only one or a few for each slab, the reader and its antenna are mounted on the moving spindle bridge, and tag ID data may be transmitted to the PLC wirelessly or by means of a wired bus. In the latter case there are some additional issues due to the movement of the spindle bridge.

Concerning the two capacitive sensing solutions we proposed in Sections 9.1 and 9.2, the experimental campaign carried out with real working conditions highlighted the main advantages and disadvantages of each approach.

As already discussed in Section 9.2, if the two sensors are realized with a comparable area occupation then the PCB-printed surface capacitor offers a reduced detection distance. Obviously, to achieve a similar detection distance the surface capacitor requires a larger area. Indeed for the marble machine application case study a total area of 220 cm^2 is required for the surface capacitive sensor in Section 9.2, 2.75 times larger than the area of the sensor in Section 9.1 which is 80 cm^2.

As far as the detection robustness is concerned it is clear that, in average, the frequency changes in Figure 30 for the surface capacitor are lower than those in Figure 25 for the single-plate capacitor suspended over the machine metallic plane. However the minimum detected frequency change value in both solutions is comparable: 2.5 kHz in Figures 25 and 2 kHz in Figure 30. Since our goal is an on/off detection of the stone samples, as previously discussed a threshold of about 1 kHz is adequate for both capacitive sensor systems in Sections 9.1 and 9.2. This allows, for both systems, sufficient margins against false or missing detections due to parasitic capacitance change, deposition of marble dust or mud, and change of temperature conditions.

The main advantages of the capacitor described in Section 9.2 versus the solution in Section 9.1 are

(i) the possibility to avoid cabling between the suspended plate and the metallic base of the marble machine;

(ii) the possibility to implement on the same PCB the capacitive sensor, the front-end measurement circuitry, and the interface for data communication (wired or wireless).

With the surface sensing approach, cabling and connection problems are reduced and system maintenance is simplified.

10.2. Case Study Application of Networked Sensing Data Collection in Marble Machines. In this section we discuss the application of the detection sensors outside and inside the machine and the concerning data generation. As application case study, we consider the surface capacitive sensors, as the collection of their output data is performed by means of an architecture resulting in an extension of the one used for the UHF RFID detection and data collection technologies applied at the machine entrance stage.

The arrangement of several sensors into a linear array implements a multipoint sensing scheme for the spatial sampling of the slab, as currently done by mechanical or optical sensors just at the entrance stage of the machine.

The linear array is mounted perpendicularly to the movement direction of the conveyer belt and spans for its entire width, see Figure 31. We indicate with w_{cb} the width of the

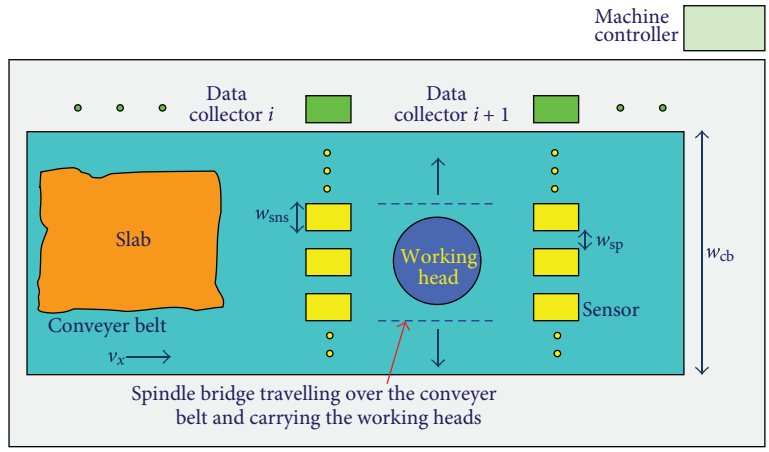


Figure 31: Schematic representation of the machine sensing and data collection architecture.

conveyer belt, with w_{sn} the width of each sensor, and with w_{sp} the spacing among two sensors in the array.

We have therefore a number of sensors n_{sns} given by

$$n_{sns} = \text{floor}\left(\frac{w_{cb}}{(w_{sn} + w_{sp})}\right). \quad (7)$$

Sensor output data have to be collected, processed, and transmitted to the machine controller, which, in case of the sensors mounted inside the machine, compares sensor data with data previously drawn from the sensors at the entrance stage, being therefore able to be aware of unexpected slab displacements.

As already mentioned in the beginning of the present Section 10.2, as a case study we consider an array of capacitive sensors usable also inside the machine.

Each capacitive sensor and the relevant front-end circuitry for oscillation generation and frequency detection implement a node of the sensing array, connected to the other sensing nodes through a wired bus (e.g., RS-485, I^2C, CAN, etc.).

For the implemented surface capacitive sensors of Figure 28, whose lower side is 10 cm long, we consider the following data:

w_{sn} = 10 cm, width of the surface capacitor PCB;

w_{sp} = 10 cm, spacing among capacitive sensors;

w_{cb} = 3.0 m, width of the conveyer belt.

We have therefore a number of sensors given by (7) which leads to $n_{sns} = 15$.

As illustrated in the schematic representation in Figure 20, we propose a surface capacitive sensor connected to a small supplementary PCB (that can be further integrated with the sensor on the same PCB) integrating an oscillator (555 timer), a low-cost 8-bit microcontroller (Atmel ATmega 16, which has been chosen for demonstration purposes and is largely sufficient in terms of the features needed), and a communication interface for multidrop bus communication that in the application case study was chosen as the I^2C bus directly driven by the microcontroller in slave mode. Of course, such a communication bus may be substituted by other industrial data buses in an on-field application. The data collector (see Figure 31) is a microcontroller-based (Atmel ATmega 16) device acting as I^2C master, reading frequency data from the different sensors and implementing proper slab detection and slab shape sampling algorithms whose results are transmitted to the machine controller.

More specifically, the microcontroller on each capacitor enables/disables the oscillating circuit, measures the capacitor oscillation frequency, and sends it every regular interval to the master microcontroller.

The slab detection and slab shape sampling strategies are devolved to the master microcontroller and not to the on-board intelligence of each sensor, as the master microcontroller is aware of the oscillation frequencies of all the sensors in the array, and can therefore

(i) detect quiescent oscillation frequency during a learning/calibration phase performed periodically (without any slab passing) or at machine start and set different detection threshold levels for frequencies of the different sensors; moreover, quiescent frequency may be quite different from sensor to sensor due to the spread in physical and electrical characteristics of its components and to the surrounding environment, for example, proximity to metallic parts of the machine, and so forth;

(ii) detect, during operations, frequency derating due to variations in the water level, in the environment temperature, and so forth, and change detection threshold accordingly.

The master microcontroller (data collector) communicates with the main machine controller wirelessly or through a wired data bus, sharing the communication channel with the other master microcontrollers managing other sensor arrays, and transmits to the machine controller detection data. Each data collector also receives commands from the machine controller, for example, to activate/deactivate sensor arrays, and so forth. The above architecture, in which

single sensor arrays and the respective data collector devices are connected to the same cables (supply and, for wired communication, to the data bus), allows for reduced cabling: in the mechanical sensors at the machine entrance stage, see Figure 3, tens of cables, one for each sensor tip, are connected to the PLC. The communication between each sensor and the array data collector occurs with a relatively low rate. In the application case study, the oscillation frequency is coded using 2 bytes (8 Hz resolution for a full scale frequency of 524288 Hz); the number of sensors for each array is $n_{\text{sns}} = 15$, and each sensor is assigned a 1-byte I^2C address; sensor data is transmitted every $T = 1$ s; the slab is transported on the conveyer belt at a $v_x = 5$ cm/s. In such a case, the obtained spatial sampling is $s_x = v_x \cdot T = 5$ cm and $s_y = w_{\text{sn}} + w_{\text{sp}} = 20$ cm.

If no transmission data integrity check or redundancy is used, the needed transmission rate is about $f_{\text{TX}} = n_{\text{sns}} \cdot 3/T = 45$ B/s, that is, well under 1 kbit/s, a communication speed reachable on commonly used data buses, even in an industrial scenario.

Of course, in an industrial, electrically noisy environment, and due to the impact on the process safety itself, it is necessary to implement data integrity check and filtering schemes, at the sensor raw data output level (a checksum byte for frequency data) and at processing level by the data collector (e.g., removing isolated detection/nondetection points near frequency threshold).

Concerning the implementation costs, a capacitive-based sensing solution could in general be less expensive than a RFID-based sensing one. As an example, a cost estimation for a RFID-based linear array sensor (UHF system, 4 antennas) leads to a cost higher than the corresponding capacitive linear array sensor. It should be anyway noticed that the price of machines for marble slab working is in the order of one to several hundreds of thousands of euros, and therefore the cost of electronics (estimation in the order of thousands of euros) would have a limited impact on the whole machine cost. Anyway, for a correct comparison of the implementation cost, also the impact on the mechanics of the machine sections involved (e.g., the metallic basement) should be evaluated by means of a detailed mechanical design review, that is beyond the scope of the present paper, but the impact appears reasonably limited in comparison to the overall machine cost. As marble machines can operate for several years, the overall cost saving due to the possibility to prevent or reduce damages to the conveyer belt and the consequent machine stops also contributes to justify the extra cost needed for the sensing application. Moreover, the RFID technology might be used not only for slab detection and process control but also to manage the marble logistics during the entire travel and stocking in the working facility, as an example in [34].

11. Conclusion

The paper has presented an experimental analysis towards the application of RFID and capacitive wireless sensing technologies to process control in the marble industry. The final aim was the detection of the presence of a marble slab under the abrasive/cutting head inside an industrial machine or outside at the machine entrance stage. The proposed techniques try to overcome issues related to currently used detection sensors: mechanical or optical devices which suffer from deterioration and dirt-related problems and do not provide the main machine controlling system with feedback signals about the correct alignment between each marble slab and the corresponding cutting/abrasive head inside the machine. This may result in safety issues, costly damages for the machine itself, and a long production stop.

The experimental results for the analyzed RFID technologies using a test setup reproducing the marble machine environment (with water, mud, marble dust) and considering more than 16 different types of stones have led to depict advantages and limits for each tested technology and to define their possibility of use at the entrance stage and/or inside the machine.

The proposed capacitive sensing solutions are optimized for the contactless detection of stone samples inside the industrial machine. Compared to the state-of-the-art detection systems, the proposed solutions allow for a reliable detection while being of low complexity and with low maintenance cost, can be easily integrated with the machine controlling system and are robust to harsh environment conditions. We have then proposed an application case study for surface capacitive sensors representative of a sensing and data collecting network architecture for slab detection outside and inside the machine, providing the machine controlling system with information about the slab position during working. Such architecture is suitable to a more general application, not limited to cutting/polishing processes in marble industry, exploiting the proposed contactless sensing techniques applied in the automation of industrial machinery.

Acknowledgments

This work has been supported by the Tuscany Region DOCUP program in collaboration with Celver Elettronica srl. Discussions with R. Massini, A. Carrafiello, and E. Valentini are gratefully acknowledged.

References

[1] Barsanti Spa, "Gangsaw TLD 60A/80A machine," 2009, http://www.barsantimacchine.it.

[2] Barsanti Spa, "LCA200 marble polishing machine," 2008, http://www.barsantimacchine.it.

[3] D. Miorandi, E. Uhlemann, S. Vitturi et al., "Guest editorial: special section on wireless technologies in factory and industrial automation," *IEEE Transactions on Industrial Informatics*, vol. 3, no. 2, pp. 95–98, 2007.

[4] Celver srl, "Archimedes optical system," http://www.celver.it/new-site/prodotti/prodotti-archimedes.asp.

[5] M. Bramanti et al., "A procedure to detect flaws inside large sized marble blocks by ultrasound," *Subsurface Sensing Technologies and Applications*, vol. 2, no. 1, pp. 1–13, 2001.

[6] M. A. Selver, O. Akay, E. Ardali, B. A. Yavuz, O. Önal, and G. Özden, "Cascaded and hierarchical neural networks for classifying surface images of marble slabs," *IEEE Transactions on*

Systems, Man and Cybernetics Part C, vol. 39, no. 4, pp. 426–439, 2009.

[7] J. D. Luis-Delgado, J. Martínez-Alajarín, and L. M. Tomás-Balibrea, "Classification of marble surfaces using wavelets," *Electronics Letters*, vol. 39, no. 9, pp. 714–715, 2003.

[8] S. A. Coker and Y. C. Shin, "In-process control of surface roughness due to tool wear using a new ultrasonic system," *International Journal of Machine Tools and Manufacture*, vol. 36, no. 3, pp. 411–422, 1996.

[9] E. Bozzi and M. Bramanti, "A planar applicator for measuring surface dielectric constant of materials," *IEEE Transactions on Instrumentation and Measurement*, vol. 49, no. 4, pp. 773–775, 2000.

[10] D. Vaccaneo, L. Sambuelli, P. Marini, R. Tascone, and R. Orta, "Measurement system of complex permittivity of ornamental rocks in L frequency band," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 42, no. 11, pp. 2490–2498, 2004.

[11] S. Saponara, F. Iacopetti, A. Carrafiello, E. Valentini, L. Fanucci, and B. Neri, "Capacitive sensors for process control in industrial marble machines," in *Proceedings of the 5th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS '09)*, pp. 142–147, Rende, Italy, September 2009.

[12] B. Osoincah, "Proximity capacitive sensor technology for touch sensing applications," Freescale White Paper, 2007.

[13] S. Saponara, F. Iacopetti, A. Carrafiello, L. Fanucci, B. Neri, and R. Massini, "Experimental analysis towards the application of RFID technologies in industrial marble machines," in *Proceedings of the 5th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS '09)*, pp. 67–71, Rende, Italy, September 2009.

[14] I. Ar and Y. S. Akgul, "A generic system for the classification of marble tiles using Gabor filters," in *Proceedings of the 23rd International Symposium on Computer and Information Sciences (ISCIS '08)*, pp. 1–6, October 2008.

[15] J. Martínez-Alajarín, J. D. Luis-Delgado, and L. M. Tomás-Balibrea, "Automatic system for quality-based classification of marble textures," *IEEE Transactions on Systems, Man and Cybernetics Part C*, vol. 35, no. 4, pp. 488–497, 2005.

[16] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, John Wiley & Sons, 3rd edition, 2010.

[17] RFIDline, "RFid project: special technology on marble and granite," 2007, http://www.rfidstone.com.

[18] R. Wessel, "Italian stone supplier uses RFID to track marble, granite," RFIDJournal, 2007.

[19] K. Kwon, J. Ryu, J. Sohn, and I. Chung, "Intelligent process control system with RFID cuboid," in *Proceedings of the 11th International Conference on Electronic Commerce (ICEC '09)*, pp. 1–8, Taipei, Taiwan, 2009.

[20] G. Fenu and P. Garau, "RFID- based supply chain traceability system," in *Proceedings of the 35th Annual Conference of the IEEE Industrial Electronics Society (IECON '09)*, pp. 2672–2677, November 2009.

[21] B. S. Choi, J. W. Lee, and J. J. Lee, "An improved localization system with RFID technology for a mobile robot," in *Proceedings of the 34th Annual Conference of the IEEE Industrial Electronics Society (IECON '08)*, pp. 3409–3413, November 2008.

[22] EM Microelectronic, "EM4102 Read only contact less identification device," 2005.

[23] PSION Teklogic, "Workabout Pro guide," 2004.

[24] CAEN SpA, "A928 long range UHF reader data sheet," 2007, http://www.caen.it/rfid.

[25] Open 2.4 GHz RFID Sputnik, http://www.openbeacon.org.

[26] Y.-C. Choi, M.-W. Seo, Y.-H. Kim, and H.-J. Yoo, "A multi standard 13.56 MHz RFID reader system," in *Proceedings of the International Technical Conference on Circuit/System, Computers and Communications (ITC-CSCC '08)*, pp. 1073–1076, 2008.

[27] N. Choi et al., "Design of a 13.56 MHz RFID system," in *Proceedings of the 14th International Conference on Advanced Communication Technology (ICACT '12)*, pp. 840–843, 2006.

[28] Beijing Hongchangtag Tech-Sci Development Inc, "HCT-HFR-80507," 2012, http://www.hongchangtag.com/product.asp?id=15&f1id=1&f2id=19&f1=3.

[29] M. Chaplin, "Water structure and science; water and microwaves," http://www.lsbu.ac.uk/water.

[30] M. Kollar, "Measurement of capacitances based on a flip-flop sensor," *Sensors & Transducers Magazine*, vol. 35, no. 8-9, pp. 1–7, 2003.

[31] G. Brasseur, "Design rules for robust capacitive sensors," *IEEE Transactions on Instrumentation and Measurement*, vol. 52, no. 4, pp. 1261–1265, 2003.

[32] L. Fanucci, S. Saponara, and A. Morello, "Power optimization of an 8051-compliant IP microcontroller," *IEICE Transactions on Electronics*, vol. 88, no. 4, pp. 597–600, 2005.

[33] D. Dugdale, *Essentials of Electromagnetism*, The Macmillan Press, London, UK, 1993.

[34] F. Marco, System and method for a plant for working natural stones. European Patent Application 10425405.7, 2010.

Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2012, Article ID 534512, 19 pages
doi:10.1155/2012/534512

Review Article

Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid

Sergio Saponara and Tony Bacchillone

Dipartimento Ingegneria dell'Informazione, University of Pisa, Via G. Caruso 16, 56122 Pisa, Italy

Correspondence should be addressed to Sergio Saponara, sergio.saponara@iet.unipi.it

Received 16 July 2012; Revised 13 November 2012; Accepted 18 November 2012

Academic Editor: Gildas Avoine

This paper discusses aims, architecture, and security issues of Smart Grid, taking care of the lesson learned at University of Pisa in research projects on smart energy and grid. A key element of Smart Grid is the energy home area network (HAN), for which an implementation is proposed, dealing with its security aspects and showing some solutions for realizing a wireless network based on ZigBee. Possible hardware-software architectures and implementations using COTS (Commercial Off The Shelf) components are presented for key building blocks of the energy HAN such as smart power meters and plugs and a home smart information box providing energy management policy and supporting user's energy awareness.

1. Introduction

Smart Grid is the evolution of the current power grid, into a new smarter network [1, 2]. It is a modernization, a reengineering of the electricity delivery system, through the exploitation of information and communication technologies (ICT) for power system engineering. The result should be an intelligent network that can monitor, protect, and optimize the operation of all its nodes, from the central and distributed generator layer to the end users [3–6]. The primary purpose of this innovation is to increase energy efficiency, reliability, and sustainability to address the growing electricity demand and to mitigate the climate changes reducing gas emissions. Thanks to continuous monitoring of all power grid nodes and the interconnection with classic ICT networks, Smart Grid may be used to increase the energy awareness of the society suggesting and stimulating "green behaviors."

This paper discusses aims, network architecture, and security/privacy problems of a Smart Grid in Section 2. Moreover some solutions are proposed in order to define a high-level architecture implementing privacy and security techniques in the grid.

From an ICT point of view a Smart Grid is a "network of networks" including wide area network (WAN), local area network (LAN), and home area network (HAN), going from the energy generation side to the customer's premises side. Particularly, a proper design of the HAN must ensure both customers' privacy and energy efficiency of the system. Sections 3 and 4 focus on a possible realization of an energy HAN, following the recommendations of the SEAS (Supporting Energy Aware Society) proposal by a team of Italian institutions. The aim of SEAS is the development of a high-level architecture to realize a HAN, that allows users to control their energy consumption remotely and to optimize the activities of the appliances within the network. After discussing a possible energy HAN topology, which exploits the ZigBee protocol for wireless node connectivity, the hardware architecture of the main building nodes is discussed (smart meters [7] and plugs plus a home smart information box providing energy management policy and supporting user's energy awareness). Possible implementations of such nodes, based on COTS (Commercial Off The Shelf) components, are also presented.

2. Smart Grid Aims, Architectures, and Security

2.1. Limits of Existing Power Grid and Challenges of Smart Grid. The typical structure of the existing power grid is

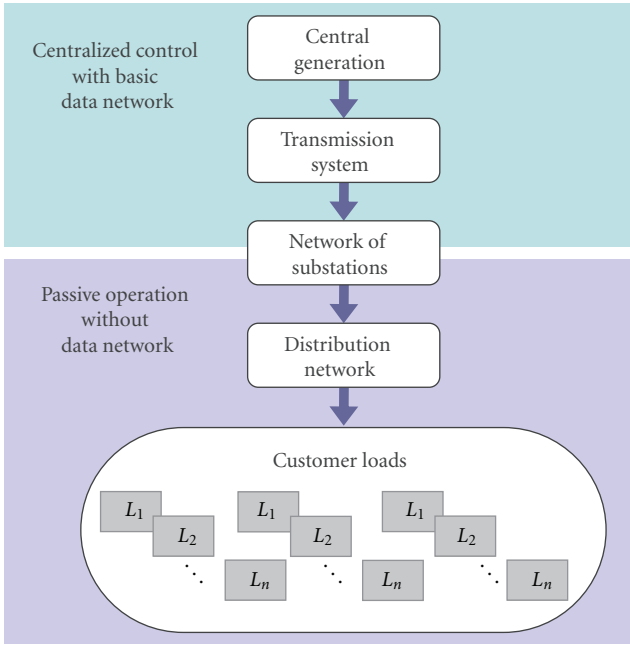


Figure 1: Structure of existing power grid.

shown in Figure 1. Utility companies all around the world designed their power grid imposing clear demarcation between its main subsystems: generation, transmission, and distribution systems. This approach has brought different levels of automation in the various subsystems, and each subsystem has separately experienced different evolutions and transformations. Moreover, the hierarchical structure of the grid can cause domino effect failures.

In term of efficiency, along the existing grid there is waste of energy in various forms: only one-third of fuel energy is converted into electricity (and waste heat is not recovered), 8% of the produced energy is lost along transmission lines, and 20% of the generation capacity exists only to support a potential peak demand [1]. This last point is very important. The existing grids are actually over-engineered to stand maximum peak demand, that are very infrequent, limiting therefore the whole system efficiency.

Moreover, present electricity grids are mainly unidirectional: generators produce energy and distribute it to the lower level, with very few information about grid status and end users energy consumption. Typically, the electric power source has no real-time information about service parameters of termination points and cannot control energy production according to the real request of the grid. The new challenges for present grids can be summarized in five main points.

(i) Introduction of new forms of power generation, in particular those using renewable energy sources such as wind, sun, and biomass. These type of generators have intermittent and small outputs and need therefore a different management from traditional generators.

Table 1: Smart Grid innovations versus existing power grid.

Existing grid	Smart Grid
Electromechanical	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Hierarchical	Network of networks
Few sensors	Sensors throughout
Blind	Self-monitoring
Manual repairing	Self-healing
Failures and blackouts	Adaptive and islanding
Manual check/test	Remote check/test
Limited control	Pervasive control
Few customer choices	Many customer choices

(ii) Need of uninterrupted electricity supply.

(iii) Need to decrease peak demands during the day and to reduce energy waste to ensure adequate energy reserves.

(iv) Diffusion of new digitally controlled devices able to change the behavior of the electrical load (e.g., switching itself on or off), smart power meters, and energy control units implementing energy management strategy and improving energy awareness of users.

(v) Security threats, that involve not only the electricity supply but also cyber attacks [8, 9].

The evolution towards the Smart Grid begins with innovations in the existing grid by incorporating new ICT technologies in many point of the infrastructure. Table 1 shows the main differences between existing grids and Smart Grid. The starting point of this revolution is the bottom layer of the system, the electrical distribution subsystem. The first step is the insertion of distributed and networked monitoring and control systems in the electrical grid. Such systems can assist utility companies in grid monitoring and can identify potential risks, taking corrective actions in time. Secondly a complete overhaul of the ICT infrastructure is required. Communication and data management will provide a layer of intelligence over both the existing grid and the future infrastructure, allowing the introduction of new applications. This organic growth of the grid allows companies to gradually shift old grid's function into the new grid and consequently to improve their critical services.

The change of the unidirectional approach of the classic power grid with the bidirectional one introduced by the Smart Grid concept can favour the diffusion of distributed generators or cogenerators, along the existing grid. Indeed, Smart Grid can provide an easier integration of alternative sources of energy (i.e., sun, wind, etc.) characterized by time-varying energy production level with storage systems, in order to fill the gap between when/where the energy is produced and when/where the energy is required. Smart Grid can aid utility companies to make a more efficient use of the existing infrastructures, introducing step by step some

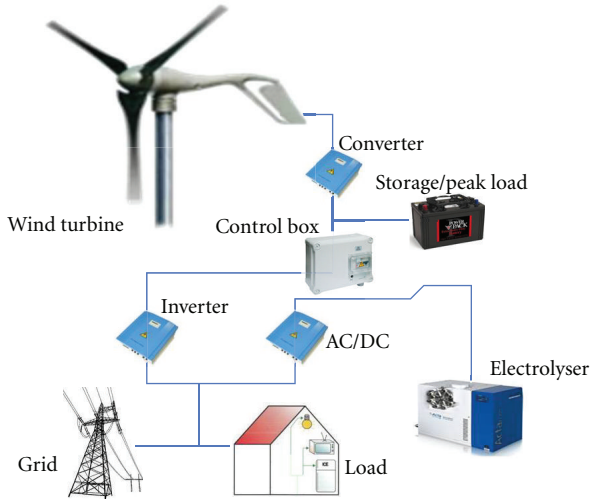


Figure 2: NanoCatGeo microgrid developed at University of Pisa.

key features as demand response, peak shaving, and service quality control [1].

The evolution of the grid requires the coexistence between Smart Grid and existing grid [10]. This permits the gradual growth of the grid, increasing step by step its capacity and adding new capabilities. A way to perform this evolution is the introduction of microgrids [11] which are networks of distributed energy systems, loads, and generators, that can work connected to the grid or not. They can be, for example, houses or factories, having their own local energy source, that want to optimize their energy consumption.

An example of a microgrid has been developed at University of Pisa in the framework of the NanoCatGeo project [12] in collaboration with industrial partners such as Acta Energy and Edi Progetti, see Figure 2. The idea was to develop a micro Smart Grid for wind-based energy autonomous homes located in windy zones. In the system a wind energy source (nonconstant energy production) plus an AC/DC converter provides energy on a DC bus wherein are also connected: (i) an inverter DC/AC system to power the home or sell any excess production to the energy utility company; (ii) an AC/DC converter to supply an hydrogen electrolyzer [13] to store in the form of hydrogen any excess when the wind electrical energy production is higher than the users' needs and to obtain energy back from hydrogen when the wind energy production is lower than users' consumption. All the subsystems of this Smart Grid are interconnected (wired) through a control box, implementing energy management strategies; the control box is based on a low-power microcontroller [14, 15], for example, an 8051-like core plus RS485 and CAN interfaces.

2.2. Smart Grid Network Architecture. Smart Grid can be viewed as a network of networks, see Figure 3. Starting from the customer side, the HAN is the network of communicating loads, sensors, and appliances within the customer's premises. Customers are connected to the energy distribution level through a LAN. LAN identifies the network of smart power meters, gateways, and elements in the distribution system. Last, we find the WAN. This is the network of upstream utility assets that include power plants, substations, distributed storage, and so on. Substation gateways interface WAN and LAN networks.

2.3. Security and Privacy Problems in Smart Grid. Since the existing grid is moving from a centralized network to a dynamic peer-to-peer network, with a growing complexity, it is also becoming more vulnerable to local and global disruptions. Smart endpoints introduced into the network become portals for intrusion and malicious attacks. Moreover, Smart Grid is growing over systems not designed with security criteria, thus with significant security holes [8, 16, 17]. Security problems do not involve only cyber security aspects, but it concern also failures in the grid and protection against natural disasters. The following is a list of potential risks for a Smart Grid:

(i) the complexity of the grid increases accidental errors and possible points of intrusion;

(ii) the deployment of new technologies can introduce new issues in the network;

(iii) the presence of many network links increases potential cascading failures and gives more opportunities to compromise the system;

(iv) smart nodes can be vulnerable entry points for denial of service (DOS) attacks.

Particularly, the focus of Smart Grid security is on the HAN: indeed WAN and LAN in Smart Grid are known computer networks whose security issues are widely discussed in literature. The HAN network is deployed into the customer domain, and its security is a critical point strictly related with customer's privacy.

A typical HAN is composed of four elements.

(i) A gateway that connects the HAN network to the outside information services, in the LAN or WAN network.

(ii) The access points or network nodes composing the HAN network.

(iii) A network operating system and a network management software.

(iv) Smart endpoints, such as smart meters, displays, refrigerators, appliances, and thermostats.

So far, many technologies have been considered in order to implement the HAN by different groups and organizations. The most significant standards are ZigBee [18], Z-Wave, Insteon, and Wavenis. They are all standards for wireless networks. The main features of these standards are presented in Table 2. Talking about security, if present, similar encryption algorithms are used by them: AES and in some cases 3DES. AES is the most reliable encryption algorithm between them [9], and its implementation (hardware and software) offers better performances than 3DES. Moreover, AES encryption can be performed using ad hoc

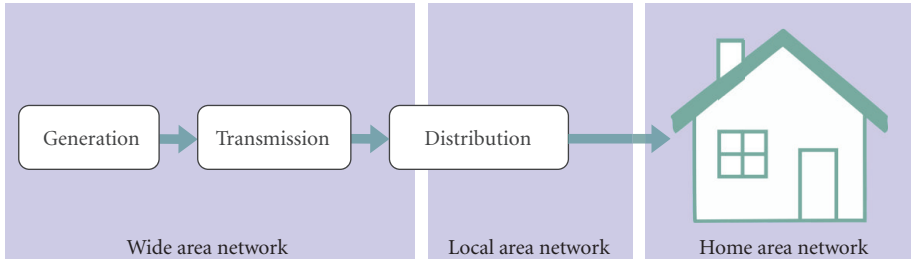


Figure 3: Smart Grid network hierarchy.

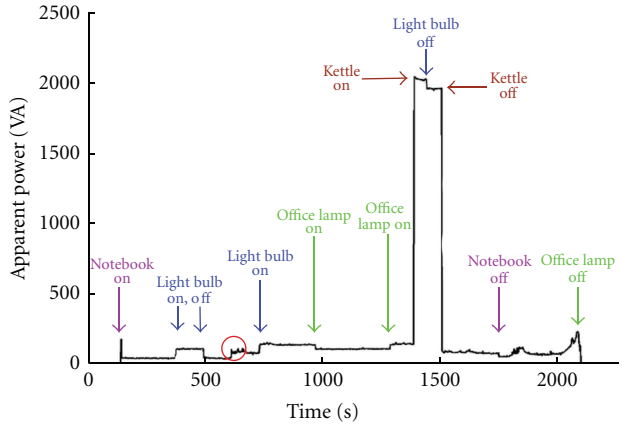


Figure 4: House electricity demand and information extracted: apparent power (Volt ∗ Ampere) for notebook, lighting sources, and a kettle [29].

Table 2: HAN standards and security algorithm, main characteristics.

	ZigBee	*Z*-Wave	Insteon	Wavenis
RF band, MHz	868/915/2400	868/908/2400	904	433/868/915/2400
Range, m	10–100	30–100	45	200–1000
Bit rate, kbps	20/40/250	9.6/40/200	38.4	4.8/19.2/100
Message size, bytes	127	64	14–28	NA
Security algorithm	128 b AES	128 b AES	NA	3DES/128 b AES

AES hardware, that is, an AES coprocessor, which is present in many of the solutions proposed for implementing HAN networks. In the example network proposed in this paper, and ZigBee standard will be used. ZigBee security issues will be discussed in detail in Section 4.

From the customer point of view, a fundamental requirement is the protection of the information exchanged between the utility company and the smart power meters installed at the customers' premises. Far from old electromechanical measuring systems, the new generation of power meters is fully electronic [19–24], and they provide advanced power measurement and management capabilities thanks to power Application Specific Integrated Circuits (ASIC) provided by semiconductor suppliers like STMicroelectronics [25]. The new generation of smart meters integrates a two-way communication system. In particular, power consumption data are transmitted over low-voltage power lines, using packet-switched digital power line communication standards [26], from the customer's premises towards data concentrators, based on Echelon technology [27]. On the other side, from each data concentrator point, information is sent to the servers of the utility company using the Internet network. Vice versa, the utility company can easily operate on remote smart meters by accessing through internet the data concentrators and from them, though power line communication over low-voltage residential power lines, the smart meters at the customers' premises. This way the utility operator can turn power on/off to customers, read usage information, change customer's billing plan, and also detect service outages or unauthorized electricity use.

Power line communication is based on the following idea. AC power is transmitted over high-voltage transmission wires at 50–60 Hz, so it is possible to impress a higher frequency signal carrying digital information in both directions (from customers' premises towards the utility company and vice versa). The carrier used for data transmission in power line communication has generally a frequency of about 100–200 kHz, for data rates of few Kbps, so that data signals can be easily separated from power ones. More details on power line communication in Smart Grid and the relevant packet formats and standards can be found in [27].

However, consumption records obtained through the smart meters can reveal a lot of information about customer's activities, thus it is important to satisfy some requirements in terms of *confidentiality*, *integrity*, and *availability*.

Confidentiality deals with information protection from unauthorized access. It is a customer side requirement. In Smart Grid, the focus is on data stored in the utility companies servers and transmitted from customer's smart meter. These data contain energy usage information and billing data. To protect them, it is important to properly implement the least privilege principle: a user has no more privileges than necessary to perform its function. A detailed guide for implementing security in the organization data server, that follows this principle, can be found in [28]. The protection of these confidential data assures customer's privacy. In fact, energy usage information reveals user

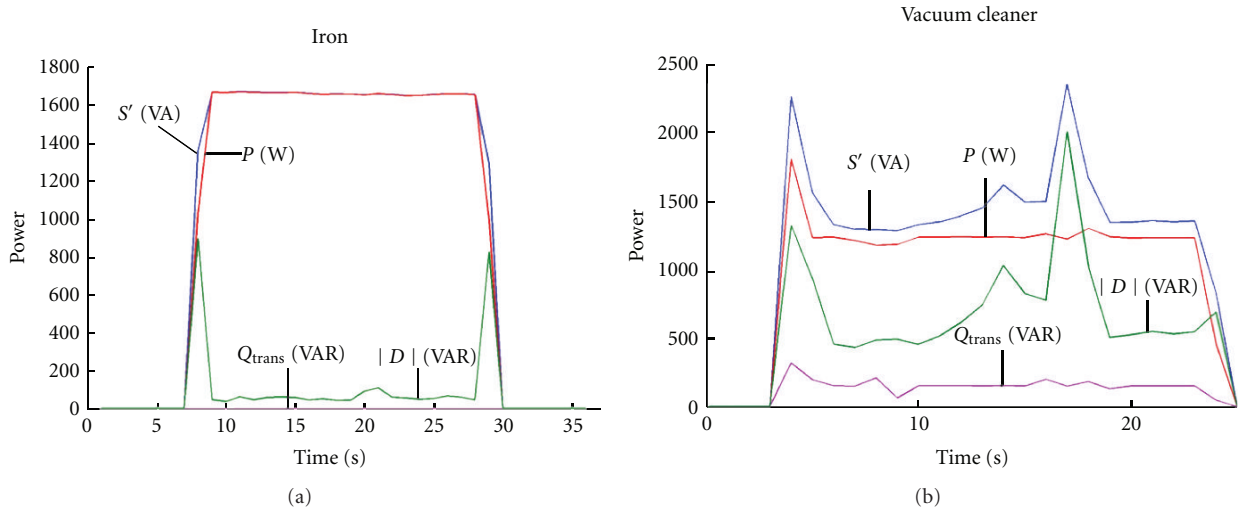


Figure 5: House electricity demand and information extracted: real power P, apparent power S, and reactive power D of an iron (a) and of a washing machine (b) [29].

activities during the day, allowing to deduce what kind of device or appliance was in use at a given time. In the literature there are a lot of load signature algorithms, results of NALM (Nonintrusive Appliance Load Monitoring) research branch [24, 29], that can extract detailed information from electricity usage records. An example of the results of these algorithms, over real consumption records, is shown in Figures 4 and 5. Signature of the usage of a specific power appliance can be extracted considering typical power consumption of the load, frequency of use, and transient response since different appliances have different load types: nonlinear resistors for heaters and bulb lamps, inductive for electric motors, reactive for microwave oven, and diode like for led lights.

Integrity ensures the correctness of information protecting data against modification attacks. A countermeasure to prevent this type of attack is based on the access control. With this, only authorized users can modify the information.

Availability ensures that services are always available to users. Security must prevent out-of-service due to human factor or DOS attack against utility companies that can compromise power distribution. Redundancy is a good practice to prevent environmental threats.

2.4. Practice to Secure the HAN in Smart Grid. In information technology, there are a lot of codes and rules in order to achieve the security requirements emphasized. An example is ISO/IEC 27000 series, a set of standards of certified best practices for information security [30–32]. Another security program, not certified, is the Information Security Forum (ISF) [33]. ISF is a nonprofit organization that distributes the Information Security Forum's Standard Of Good Practice free of charge.

These guides can be applied to ensure information security for every kind of systems, including Smart Grid and particularly for the HAN which is the main focus of this paper. A code of technical practice for security in the HAN of a Smart Grid can be summarized in the following twelve points.

(1) *Threat Modeling.* Possible threats must be identified, for preparing proper countermeasures. This study can be conducted analyzing use case versus abuse case.

(2) *Segmentation.* To minimize the impact of attacks, segmentation can be adopted limiting, for example, data traffic in specific area through a firewall: attack damage would be confined to such area.

(3) *Firewall Rules.* Proper rules must be used for firewall, proxy server, and content filtering.

(4) *Signing.* Software codes running in the grid have to implement digital signing. This allows the execution only of trusted applications and ensures integrity of the information exchanged within the Smart Grid.

(5) *Honeypots.* The deployment of honeypots, traps for hackers, permits identification of a new type of attack and alerts organizations in time. Thus, honeypots show weakness and security hole of the system. These elements can be placed in the Smart Grid environment and in its peripheral areas.

(6) *Encryption.* Through the encryption algorithm, sensitive information is protected from unauthorized disclosure. Encryption must be adopted on the transport layer, on the archived data and in the control network.

(7) *Vulnerability Analysis.* Utility companies have to create control centers to analyze network traffic and systems to identify any exposures that increase vulnerability to attacks.

(8) *Penetration Testing.* Beside vulnerability analysis, simulating an attack usually done by a malicious

Table 3: IEC 62351 core standards.

Core standard	Topics
IEC 62351-1	Communication network and system security introduction
IEC 62351-2	Glossary of terms
IEC 62351-3	Profiles including TCP/IP
IEC 62351-4	Profiles including manufacturing message specifications (MMS)
IEC 62351-5	Security for IEC 60870-5 and derivatives
IEC 62351-6	Security for IEC 61850
IEC 62351-7	Network and system management (NSM) data object models
IEC 62351-8	Role-based access control

hacker on the Smart Grid must be performed periodically; this way a snapshot of the effectiveness of the Smart Grid security can be obtained.

(9) *Source Code Review.* Smart Grid applications must present no vulnerabilities. Thus, their source code must be reviewed carefully in order to meet high-quality requirements. After the identification of vulnerabilities in the code, these can be fixed.

(10) *Configuration Hardening.* All the elements of the Smart Grid, especially smart endpoints, have to be tested before their deployment. This can be done with vulnerabilities scanners and benchmarking tests.

(11) *Strong Authentication.* There are three main types of authentication methods: something the user knows (e.g., password), something the user has (e.g., hardware key), and something the user is (e.g., biometric id). At least two of these methods must be used.

(12) *Logging and Monitoring.* They are powerful tools for providing information for attack identification and for reconstructing events in case of natural disasters. Starting from stored data, data-mining techniques and signal processing analysis give important information about attacks and grid behavior during certain events. However, if not correctly managed, data logging could represent a further backdoor into the system. For this reason it is important to define an accurate log planning process including log management planning, policies, and procedures taking into account security issues [34].

This set of practices can be also used as a backbone for the development of future Smart Grid standards.

2.5. Security Standards and Proposed Solutions for Smart Grid. Several associations and groups in different countries have developed many standards for security in Smart Grid. The IEC 62351 standard, developed by the International Electrotechnical Commission (IEC), is one of them. This standard concerns power system management and associated information exchanged and is divided in eight core standards, reported in Table 3. The scope of the IEC 62351 standard is information security for power system control operation [35]. In Table 3 other two IEC standards are mentioned: IEC 60870 and IEC 61850. The first one, the IEC 60870 standard defines system used for telecontrol. Part 5 of this standard deals with communication between nodes directly connected. IEC 61850 is an electrical substation automation standard for modelling data, reporting schemes, fast transfer of events, setting group, sample data transfer, commands, and data storage.

NIST interagency report 7628 for cyber security in Smart Grid is another important document [36]. This report contains a framework for cyber security risk management, a list of requirements for power meter security, and a discussion about privacy and Smart Grid. Moreover, this document contains power system use cases for security requirements and bottom up security analysis of Smart Grid.

Besides these standards, in literature there are some solutions and models proposed for implementing security in Smart Grid. One of the most interesting solution is based on public key infrastructure (PKI). This is based on the fact that security and privacy technologies use a key to encrypt and protect data, in order to meet the desired security requirements. The problem, in a large network as a Smart Grid, is the key management system. The PKI proposed is composed of five main elements:

(i) PKI standards;

(ii) Smart Grid PKI tools;

(iii) device attestation;

(iv) trust anchor security;

(v) certificate attributes.

PKI standards would be used to determine requirements on the PKI operations of energy service provider. PKI, however, is notoriously hard to deploy and to use, due to the fact that PKI standards provide only high-level framework, and leave to companies the detailed implementation. Smart Grid PKI tools give users an easy way to manage the infrastructure and enable the development of future applications, which meet PKI security requirements. An important feature of these tools is to eliminate the need of symmetric key configuration, which is an insecure and expensive process. In a secure system, each component must be a trusted component. Device attestation techniques are used to identify devices and to find out if the device has been tampered. Within a network based on PKI infrastructure, an important aspect is the management of devices' certificates. These certificates can be organized in trees, and the root is called Trust Anchor (TA). It is important to secure operations on TA: loading and storing, identification, management of local policy database (a set of rules defining how a device should use its certificates, and what type of certificates it should accept), and so forth. It is essential in Smart Grid that any device in the network can determine the authorization status of another device and authenticate it. This can be done using the attributes present into the certificate and contacting a security server. Therefore, it is important to distribute local security servers in various part of the network and not to rely only on a back-end server (single point of failure problem).

The solution proposed is only a high-level description of how security and privacy can be achieved in Smart Grid, and many problems may come out during the implementation of a PKI infrastructure. Some of these problems were discussed previously (i.e., need of distributed authentication servers, implementation of PKI standards, secure management of devices certificates, etc.).

Alternatively, the PAKE (password-authenticated key exchange) research [37, 38] explores an approach to protect passwords without relying on PKI at all. PAKE aims to achieve two goals. First, it allows zero-knowledge proof of the password. One can prove the knowledge of the password without revealing it to the other party. Second, it performs authenticated key exchange. If the password is correct, both parties will be able to establish a common session key that no one else can to compute.

As far as privacy of the customers is concerned, a possible solution is based on the anonymization of smart meters data. The idea is to distinguish smart meters data on the basis of their generation frequencies.

(i) High-frequency data sent by smart meters to utility data concentrators in order to control power generation and distribution network and to enable a real-time response to power quality. These data do not need to be attributable to a particular customer and are sent, for example, every minute.

(ii) Low-frequency data sent to utility company, for billing and account management. These data must be attributable to a customer or an account and are sent every day/week/month.

Only high-frequency data are "anonymized," because of their sending rate. A smart meter, using this technique, has two ID for its message: an HFID for high-frequency data, and a LFID for low-frequency data. The method proposed ensures the anonymity of the HFID, thus of high-frequency messages. The utility company and customers know only their LFID, and the HFID is known only by the manufacturer of the smart meter, that so it is the only one that has the correspondence between LFID and HFID. The HFID for example can be hardware encoded. This solution, however, considers only data sent from smart meters. The limits in terms of security of an approach similar to the proposed one (HFID and LFID correspondence is known by the smart meter manufactures and stored in its archives) are discussed in [39].

3. Home Energy Network Possible Implementation

3.1. Home Energy Network Architecture. This section presents a possible implementation of a home area network for smart energy management, discusses security issues, and analyzes some commercial hardware/software solutions for its implementation. The network proposed is derived from the experience gained in Smart Grid projects proposal in Italy such as the Energy@Home project [40], carried out by industrial partners such as Electrolux, Enel, Indesit and Telecom Italia, and the SEAS proposal, by Italian academic partners. The aim is to develop a communication infrastructure, for exchanging information related to energy usage, consumption, and tariffs in the home area network.

The general architecture of the smart energy HAN is presented in Figure 6. The HAN network contains a smart information box called Home Energy Angel, realized as an electronic control unit with on-board memory, computing capabilities (32-bit microprocessor with nonvolatile, SRAM, and SDRAM memories) and digital networking interfaces.

The Home Energy Angel box implements these main functions:

(i) collecting data from the power meters and from the smart endpoints in the home domain, monitoring the energy sources (from the electricity provider or from local renewable energy sources such as photovoltaic panels or wind-based systems), the energy loads (recharge point of electric vehicles if any, lighting, air conditioning, household appliances and infotainment devices), and the energy buffers (Li-ion batteries or H2-based energy storage [13]);

(ii) collecting data through the HAN from environmental sensors (temperature, light, and humidity);

(iii) forecasting of users' needs, based on data provided by sensors and by profiling methods;

(iv) sending commands to smart appliances according to preprogrammed strategies to implement power saving strategies (e.g., turn off/on lights adaptively on the environment conditions, proper time programming of washing machines or oven to avoid peak consumption,...),

(v) providing information to the users about their energy behavior through their tablet PC or smartphones.

Beyond the Home Energy Angel box, a home gateway is also connected to the HAN. This provides internet access for users through a Wi-Fi network. The home gateway is the interface between the HAN and the WAN network (internet in this architecture). Users can obtain information about home consumption contacting the Home Energy Angel information box through the home gateway, using a simple internet connection or locally using the connected interfaces on their tablet, laptop, or smartphone. The Home Energy Angel smart information box provides energy services to make customers aware about their energy consumption. These services are automatic load management, energy efficiency, active demand service, and networking with smart appliances.

A graphical user interface (GUI) will be developed for the Home Energy Angel, enabling a better user experience of the whole system. The GUI will be designed for two main purposes. Firstly, users will be able to easily provide information on their preferences in using the energy at home (i.e., on the appliance that they are willing to use, on the time window to start/stop each device). Secondly, it will be used to visualize the optimal energy plan calculated by the Home Energy Angel and to access additional information

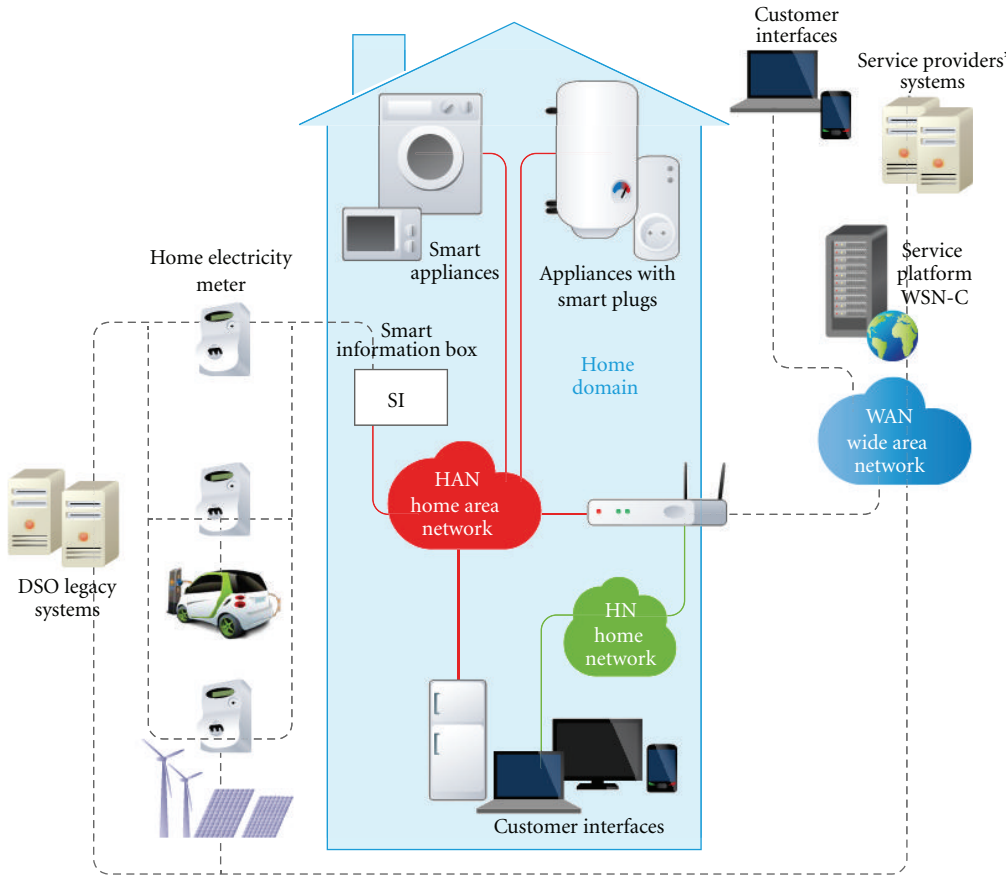


Figure 6: Smart energy HAN general architecture.

such as the load consumption profile, costs, or statistical data, thereby settling the general lack of awareness people have of their energy consumption.

The proposed Home Energy Architecture will provide benefits in terms of the following.

(i) Provide an easy-to-use support to optimize the production and consumption of electricity, reduce electricity cost, and minimize electricity waste.

(ii) Increase user awareness on energy consumption/saving.

(iii) Improve the grid efficiency by leveling peaks in the demand.

Energy consumption information, collected by meters, can be sent directly to the Distribution System Operator servers (DSO legacy systems in Figure 6) exploiting power line communication protocol instead of using the HAN connection.

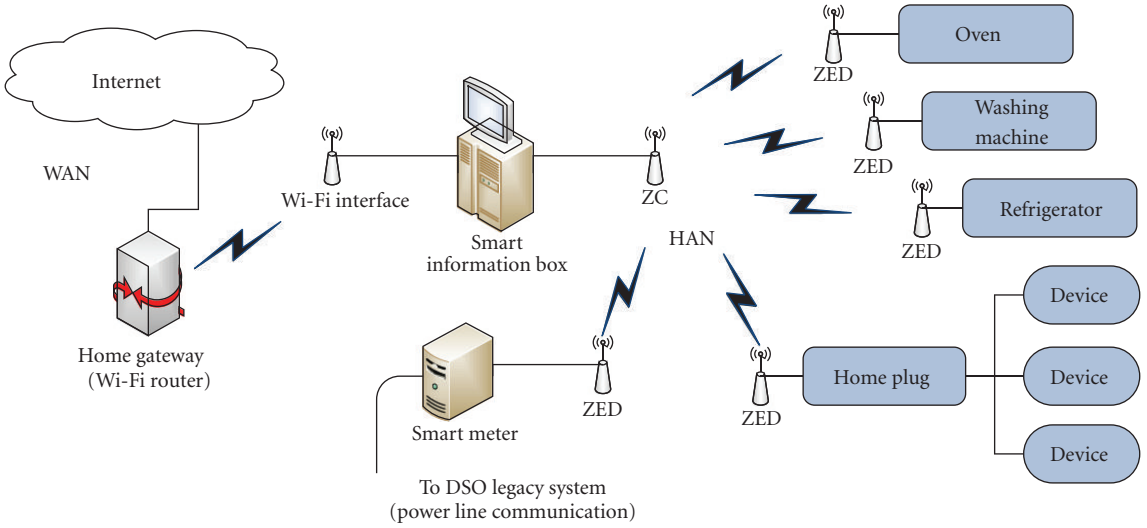
In the architecture detailed in Figure 6 there is another particular element: the smart plug. Smart plugs (or home plugs) are systems able to add intelligence to old generation devices. They are simple socket points with a wireless connection (e.g., ZigBee) providing consumption monitoring of the connected devices. Smart plugs can also control the status of the connected devices (powering them on/off, i.e., are intelligent power switch [41]) sharing the power among them.

The system architecture of the network is shown in Figure 7. A possible implementation of this system uses a ZigBee network for realizing the HAN. Within the network there is a smart information box, connected to the HAN through a ZigBee transceiver and equipped with a Wi-Fi interface for contacting the home gateway. The home gateway is a simple Wi-Fi router. The role of the smart information box is to collect data from the HAN to compute them using information coming from the internet network (customer's tariff, billing account information) and to present them by means of a user-friendly interface.

The home gateway acts as an interface between the WAN (internet) and the HAN. A Wi-Fi router can play this role: the smart information box can be accessed remotely from users and can easily contact the utility service servers. In the example of Figure 7 there are four smart appliances: an oven, a refrigerator, a washing machine, and a smart plug; together with the smart information box and the smart meter transceiver, they form the HAN.

ZigBee protocol assigns a role to each node into the network. There are three possible roles.

(i) ZigBee coordinator (ZC): it is the smartest device in the network. The coordinator node is the root of



ZED: ZigBee end device.
ZC: ZigBee coordinator.

Figure 7: Smart energy HAN architecture implementation example.

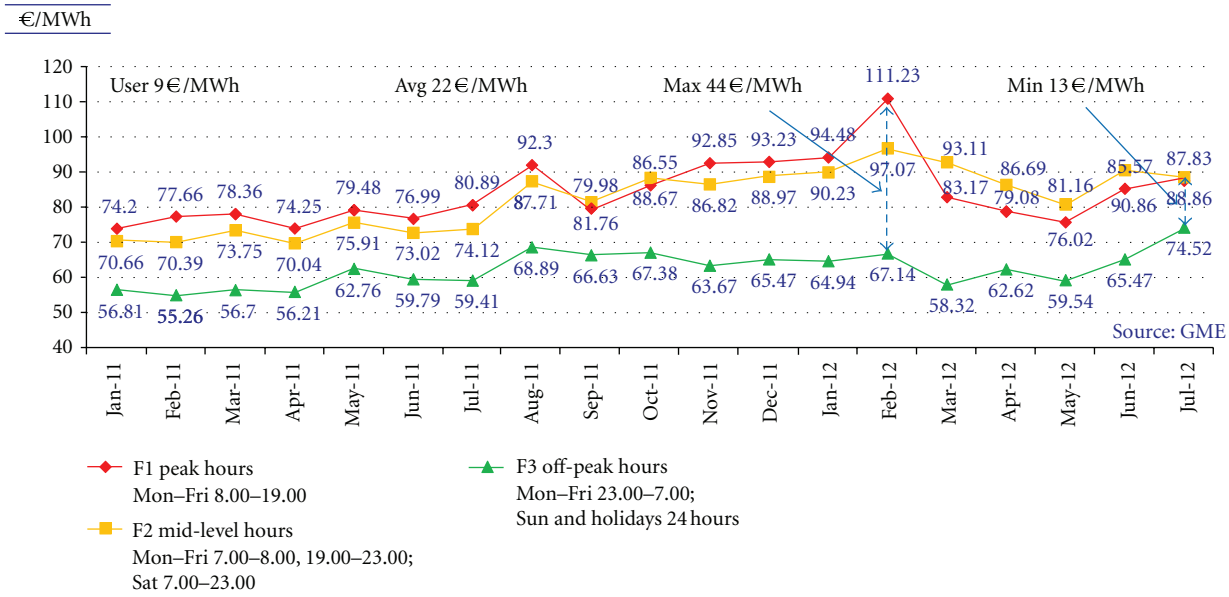


Figure 8: Cost of energy in different time ranges in Italy.

the network and can also act as a bridge between different networks. It can contain information about the network as well as store the security keys. In each ZigBee network there is only one coordinator. The smart information box is the ZC of the example network of Figure 7.

(ii) ZigBee router (ZR): it acts as router in the network, exchanging data between nodes (not present in the example network of Figure 7).

(iii) ZigBee end devices (ZEDs): they are the simplest nodes of the network, and they can communicate only with the coordinator or routers. ZEDs require little amount of memory. The devices in the network of Figure 7 are all ZEDs, and they communicate only with the smart information box.

It is worth noting that ZigBee is not a protocol for peer-to-peer networks (i.e., networks composed by nodes that have all the same role and where there is no distinction between them). ZigBee instead assigns a role to each node, and ZEDs cannot communicate directly, but only through a router or coordinator. Using routers within ZigBee network allows the deployment of a network architecture similar to mesh network.

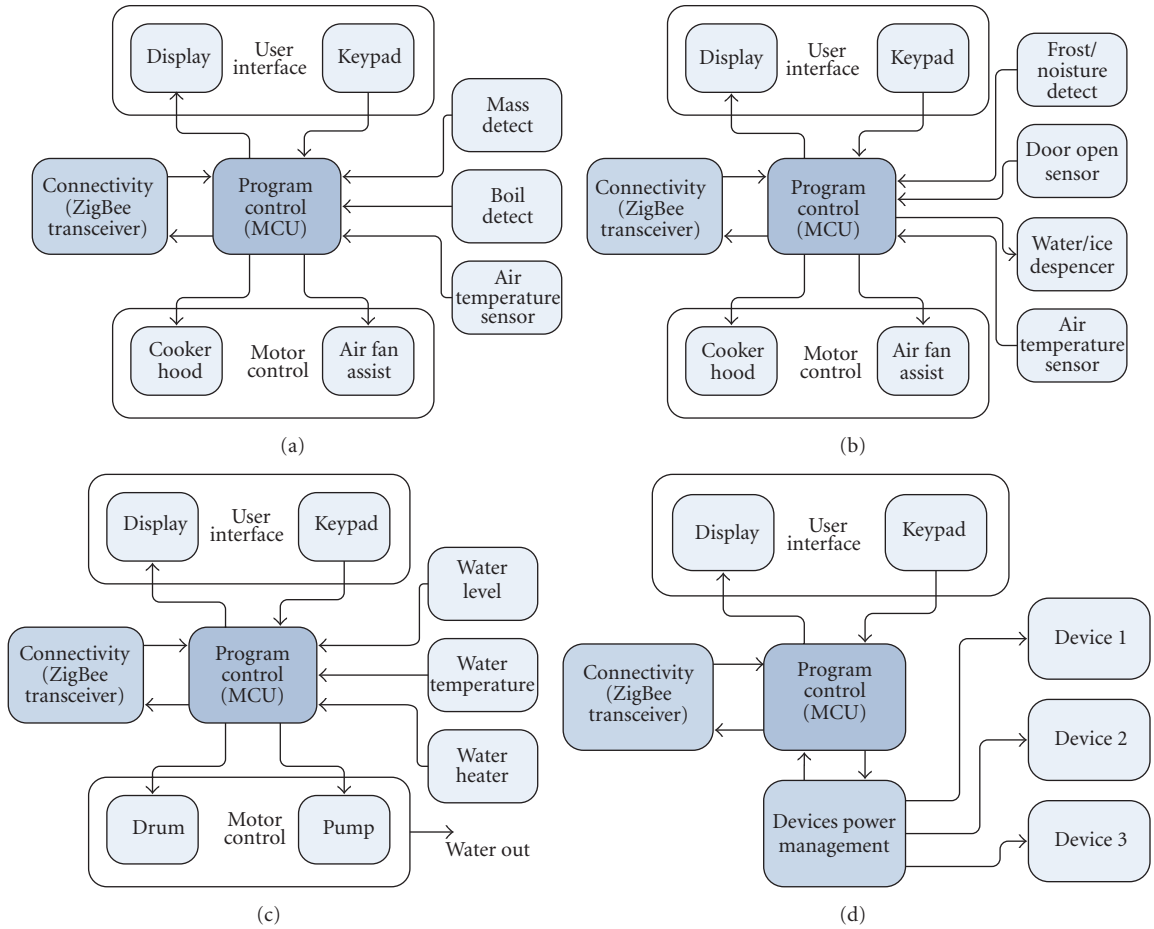


Figure 9: Oven (a), refrigerator (b), washing machine (c), and home plug (d) system diagram.

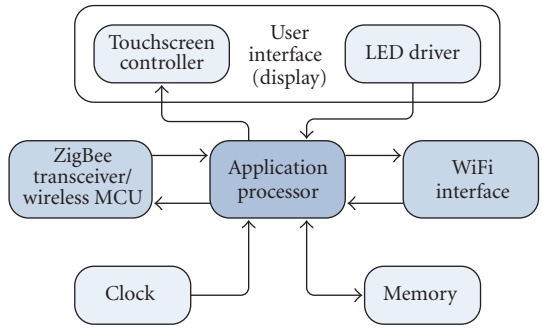


Figure 10: Architecture of the Home Energy Angel smart box.

Moreover the Home Energy Angel in our vision is a smart device that runs applications specific for energy management. It is a point of presence for every smart device within the home domain and for third party's domotic solutions. For our purpose, the Home Energy Angel smart information box can integrate also the Wi-Fi router to provide an internet access to users. In such a case all the applications for network and energy management run on the Home Energy Angel smart information box, that acts also as a gateway.

Implementing the proposed energy HAN will allow energy saving and cost saving benefits for the end users.

As discussed at the last SustainIT2012 conference in several papers [42–44] in Europe the household contribution to the overall electricity consumption is about 29% corresponding for a country like Italy [44] in 70 TWh per year, 12 billions of Euros of cost, 2.5 MWh/user per year. Simulations carried out considering the power cost of typical house appliances, and the consumption profiles of typical users allow the following estimation: the introduction of

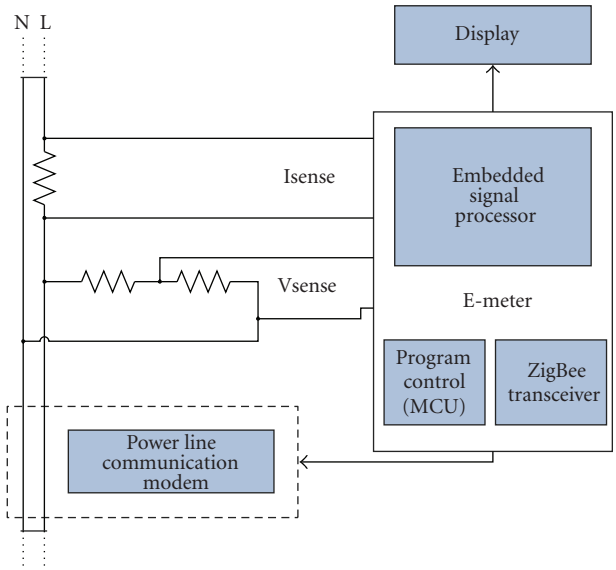


Figure 11: Architecture of the smart meter.

the energy HAN, supporting energy awareness of users, and implementing automatic energy management policy can reduce the user consumption per year by 20% from actual 2.5 MWh to 2 MWh.

A further cost saving can be achieved, thanks to the HAN, by enabling users to automatically exploit the high variability of energy cost which, as reported in Figure 8, can vary by a factor 3 from peak hours (F1 tariff in red in Figure 8) to off-peak hours (F3 tariff in green in Figure 8).

3.2. HW Architectures of Building Nodes: Smart Plugs, Home Energy Angel Box, and Smart Power Meters. Figure 9 shows the block diagrams of smart devices present in the example network. Every device has a microcontroller (MCU) core, for example, a 32-b RISC Cortex managing system activities, and an interactive user interface. The connectivity module enables them to join the network and to be remotely controlled. This subsystem can be a simple transceiver integrated with the MCU in the same PCB board, or a single-chip wireless microcontroller can be used.

An example of stand-alone ZigBee transceiver is the Texas Instruments CC2520. In the solution that integrates the wireless microcontroller and the transceiver in the same chip, the antenna can be directly printed on the PCB board achieving enough gain with a limited size, as demonstrated by recent works done at University of Pisa where multiloop multifrequency antennas have been realized as PCB-printed antenna for sub GHz applications [45, 46].

Both solutions can be used to upgrade the existing device's design enabling them to join home area networks. If we use a transceiver, the existing microcontroller could be connected to it using GPIO (general purpose input/output) and SPI (serial peripheral interface) lines. However, this introduces an overhead to the device MCU, that now has to control the system and to implement the communication protocol. On the other hand, using a wireless microcontroller avoids this problem. Actually, a wireless microcontroller can be used as coprocessor, placing it side by side with the device MCU in charge of the system control. The wireless microcontroller implements the communication protocol and manages the transmission and the reception of packets, while the other MCU continues implementing the control algorithm, and when it needs to communicate with other devices in the network it sends a request to the wireless microcontroller. The overhead introduced by this scenario is limited.

The architecture of the Home Energy Angel smart information box is shown in Figure 10. A touchscreen display (in-home display) provides an easy way for users to interact with the smart box. Through this display the user can manage the energy settings of the devices connected to the HAN network and can check the energy consumption records. An external permanent memory is needed to store past records, files for software running on the smart information box and any significant information about the network. The smart information box needs a connection to internet in order to retrieve information about customer energy account, that are used by energy management applications. For that reason there is a Wi-Fi interface connected to the device MCU.

Figure 11 presents the block diagram architecture for the smart meter to be installed by utility companies (e.g., ENEL in Italy). The core of the smart meter is represented by the electronic meter (E-meter), able to calculate the energy consumption by sensing current and voltage from the electric network through an analog front end. This information is digitized and elaborated by an MCU equipped with digital signal processing capabilities (e.g., a 32-bit Cortex processor), and then presented through a display. Also a power line communication modem is connected to the meter in order to send usage information to data concentrators. The extension required with respect to the current state of the art is the ZigBee transceiver. This component enables communication with the smart information box, so users can check their real-time consumption. The smart meter can also store consumption data into its memory for later use.

The described smart meter is the result of an evolution started from AMR (automated meter reading) systems. These meters allow utility companies to read consumption records, status, or alarms occurred. AMRs provide only one-way communication: utility companies cannot take corrective actions on the customer grid.

The evolution of AMR is the AMI (advanced metering information) meter whose hardware architecture has been detailed in Figure 11. AMI is characterized by a built-in two-way communication system, allowing the modification of customers' service level parameters. In this way customers can control energy cost choosing between different billing plans. However, as recognized in the state of the art, deploying a high number of smart meters in the environment is cumbersome. To reduce the number of deployed power metering devices without affecting the information reliability new approaches have been investigated, that is, load disaggregation for extracting individual appliance power consumption information from single-point circuit-level measures. Such approach is based on the observation that

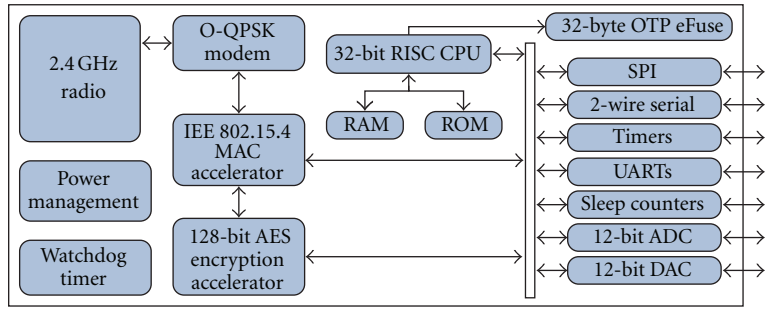


Figure 12: SoC architecture for wireless sensor networks in energy HAN.

each appliance has its own power consumption profile over time, as proved in Figures 4 and 5, which can be isolated from the single-point measure. Disaggregation aims to extract the signatures of the different appliances from the aggregate measures. With respect to the state of the art, where artificial neural networks [47] or a Bayesian approach [48] have been used to perform the appliance recognition, we aim at avoiding the training phase. To this aim we propose adopting a coarse description of the appliance "energy signatures" (i.e., how each type of appliance works and therefore its power consumption in any possible state) and recognize most of the appliance types used in a residential building by indentifying which unit is active, how long and how much is consuming. To this aim, the advanced hardware architecture proposed in Figure 11 is needed, since both a smart analog front end for the power meter measure (E-meter) and a powerful processing unit (the embedded signal processor) are required to implement the disaggregation DSP algorithms. Moreover the smart meter supports communication by wireless connection with the home area network and by power line communication with the main energy grid.

For antitapering reason a 3-axis tilt sensor is also integrated in the smart meter architecture and is connected to the Zigbee and the power line communication interfaces (i.e., if the smart meter is tampered, the end user and/or the utility is notified), see [49]. A detailed review of antitampering techniques for smart meters is reported in [50].

3.3. COTS Components Selection to Build the Energy HAN. Table 4 presents a selection of COTS components suitable for developing devices capable of forming a ZigBee network, according to the architectures presented in the previous sections. They are systems-on-chip (SoCs) integrating at least a ZigBee transceiver, on-chip nonvolatile memory, RAM memory, and a CPU with a security AES coprocessor (see on-chip architecture in Figure 12).

As far as the RF part is concerned all devices in Table 4 implement the ZigBee physical layer at 2.4 GHz with a transmitted power in the order of few mW (3–4.5 dBm being 0 dBm = 1 mW) and a sensitivity from −95 to −101 dBm. Hence considering a full TX-RX link the proposed devices can face path losses up to −100 dB which is enough to build reliable home area networks according to the topology discussed in Sections 3.1 and 3.2. Since 2.4 GHz is a worldwide unlicensed frequency, this allows the use of these transceivers in every country, without difficulties. By using an integrated MURATA antenna, printed on the PCB board, 3 dBm of TX power allows reaching 30 meters indoor/urban or 100 meters and more outdoor line of sight. As discussed in [51], several strategies are foreseen in ZigBee in order to solve frequency coexistence problems with other communication technologies (e.g., Wi-Fi, Bluetooth) in the crowded 2.4 GHz frequency spectrum.

As far as the power consumption is concerned it is in the order of several tens of mW in RX or TX active mode; by implementing power cycling strategies, the power consumption can be kept as low as few μW using the STM32W108C8 device which moreover has a short wake up time of 110 μs. To implement smart metering or energy management function devices with a 32-bit CPU have to be preferred and with both RAM and Flash (rather than ROM) on-chip capabilities. To this aim we have selected for the implementation the STM32W108C8 which has 8 kbytes and 64 kbytes or RAM and Flash, respectively, and a-32 bit Cortex M3 processor which has a computation efficiency of 1.25 Dhrystone MIPS/MHz, enhanced instructions such as Hardware Divide, Single-Cycle (32 × 32) Multiply, Saturated Math Support, and 149 μW/MHz when realized in 180 nm CMOS technology. Some of the typical MAC operations required during communication (such as ACK management, automatic back-off delay, and packet filtering) are implemented via hardware, in order to meet the strict timing requirements imposed by IEEE 802.15.4-2003 standard.

When optimizing the network, a specific customization can be done according to the specific device under control. For example, to control simple power appliances like oven, refrigerators, boiler, lights, or air conditioning, it is not needed a continuous control. They have to send their consumptions, alerts in case of troubles (oven overheat during cooking, failures in refrigerator's components, etc.), and the capability of turning on or off them remotely is needed. For these devices a simple transceiver can be added, and hence the overhead introduced is minimum. These devices have only to transmit and to receive messages at low rate: their status, including energy usage, is checked few times in a day (4/5 times in a day), and alerts do not occur frequently. So a RF transceiver can be added to the MCU already present in such machines, or their MCU can be replaced with a wireless SoC such as the STM32W108C8.

Table 4: COTS components to implement the energy HAN nodes.

Device	ATZB-24-A2/B0 [56]	JN5139	JN5148	STM32W108C8	CC2530
CPU	8 b RISC ATMega128	32 b RISC	32 b RISC	32 b RISC Cortex3	8 b RISC 8051
Radio freq.	2.4–2.485 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.394–2.507 GHz
Flash/ROM	128 kB Flash	192 kB ROM	128 kB ROM	64 kB Flash	32, 64, 128, and 356 kB Flash
RAM	8 kB	8 kB	128 kB	8 kB	8 kB
Data rate	250 kbps	250 kbps	250, 500, and 667 kbps	250 kbps	250 kbps
V supply	1.8 V–3.6 V	2.2 V–3.6 V	2 V–3.6 V	2.1 V–3.6 V	2 V–3.6 V
RX current	19 mA	34 mA	17.5 mA	27 mA	24 mA
Tx current	18 mA	34 mA	15 mA	31 mA	29 mA
Standby current	6 μA	1.3 μA	1.25 μA	0.8 μA	0.4 mA
Wakeup time	N.A.	N.A.	840 μs	110 μs	600 μs
RX sensitiv.	−101 dBm	−97 dBm	−95 dBm	−99 dBm	−97 dBm
TX power	3 dBm	3 dBm	3 dBm	3 dBm	4.5 dBm

In case of smart plug (e.g., turn on/off control of lights) where a microcontroller is not present (since no logic control is required) a simple transceiver is added without any CPU core.

When dealing with other appliances such as washing machines or rechargeable systems for electric vehicles, a continuous control can be useful to program their work and hence to find an optimal trade off between user needs, time-based energy tariff, and production peaks of renewable home energy generators (wind, photovoltaic), if any. A smart washing machine can be programmed to work during low cost time slots. To do this, once the device is programmed, it must be in standby mode until the job can be performed. Small standby consumption is required. The smart information box of Figure 10 can contact the washing machine when the low cost slot begins. Then the device can start its work. A good solution to implement the smart washing machine could be the STMicroelectronics STM32W108C8, mainly thanks to its low consumption of current during standby mode (0.8 μA). It could be envisaged the possibility to use this wireless microcontroller also to manage washing machine operations, for those models that are not too complex. Finally for the Home Energy Angel smart information box and for the smart meter with local processing capabilities (data disaggregation), powerful architectures are needed. As example in the smart meter, the STM32W108C8 SoC could just implement a part (the MCU and the wireless transceiver) of the architecture of Figure 11. The board of the smart meter should be equipped also with a display driver, an E-meter ASIC, a power line communication modem chipset, and a touchscreen/display controller. In the case of the Home Energy Angel also a Wi-Fi communication controller is needed. The ST7590 IC can be used as the power line communication modem. This device is able to operate at 28.8 kbps, and its architecture is reported in Figure 13.

For the E-meter, the ASIC reported in Figure 14 by STMicroelectronics can be used. It implements measures of active, reactive, and apparent energy by acquiring voltage or current value through dedicated acquisition channels. The accuracy is 0.1% of full scale value.

3.4. Security in the Proposed ZigBee/802.15.4 HAN. All the devices discussed in the previous section contain an AES dedicated processor to implement ZigBee/IEEE 802.15.4 secure communications. AES is the encryption algorithm used in the proposed network. On-chip one time programmable memory can be used to store 64-bit MAC ID and 128-bit AES security key. As reported in Figure 15, with respect to the ISO/OSI protocol stack, ZigBee implements the first three layers (application, transport, and network layer), while IEEE 802.15.4 provides protocols for data link layer (i.e., divided in logical link control and media access control). This standard has several versions, named by year. The most important are the 2003 and 2006 versions. IEEE 802.15.4 uses 27 channels divided in three main bands; the most interesting are the 16 channels available in the worldwide available 2.4 GHz unlicensed band. To avoid the simultaneous transmission of several nodes, the standard uses CSMA-CA (Carrier Sensing Multiple Access-Collision Avoidance) or GTS (Guarantee Time Slots) protocol. A node using the CSMA-CA protocol, before sending packets in the network, checks if the communication medium is free or not: if the medium is free the node will send its packets, otherwise the node will wait for a certain period of time, computed with specific back-off algorithms (e.g., exponential back-off algorithm). The GTS protocol, instead, uses a coordinator node which gives to the other nodes time slots, so that anyone knows when it has to transmit its data. An interesting feature of IEEE 802.15.4 is the channel energy scan. Before using a channel, network sees how much energy (other network activity, noise, and interference) there is.

This mechanism saves energy, choosing free channels when setting the network. IEEE 802.15.4 is a low consumption protocol. Nodes that use this protocol can keep their transceiver sleeping most of the time (up to 99%), and receiving and sending tasks can be set to take small part of the devices' energy. ZigBee [18] is a standard for high-level communication based on IEEE 802.15.4 [52–55] data link standard. ZigBee is widely used in short range wireless communications requiring low date rates, low energy consumption, and a secure channel. The standard offers four main services.

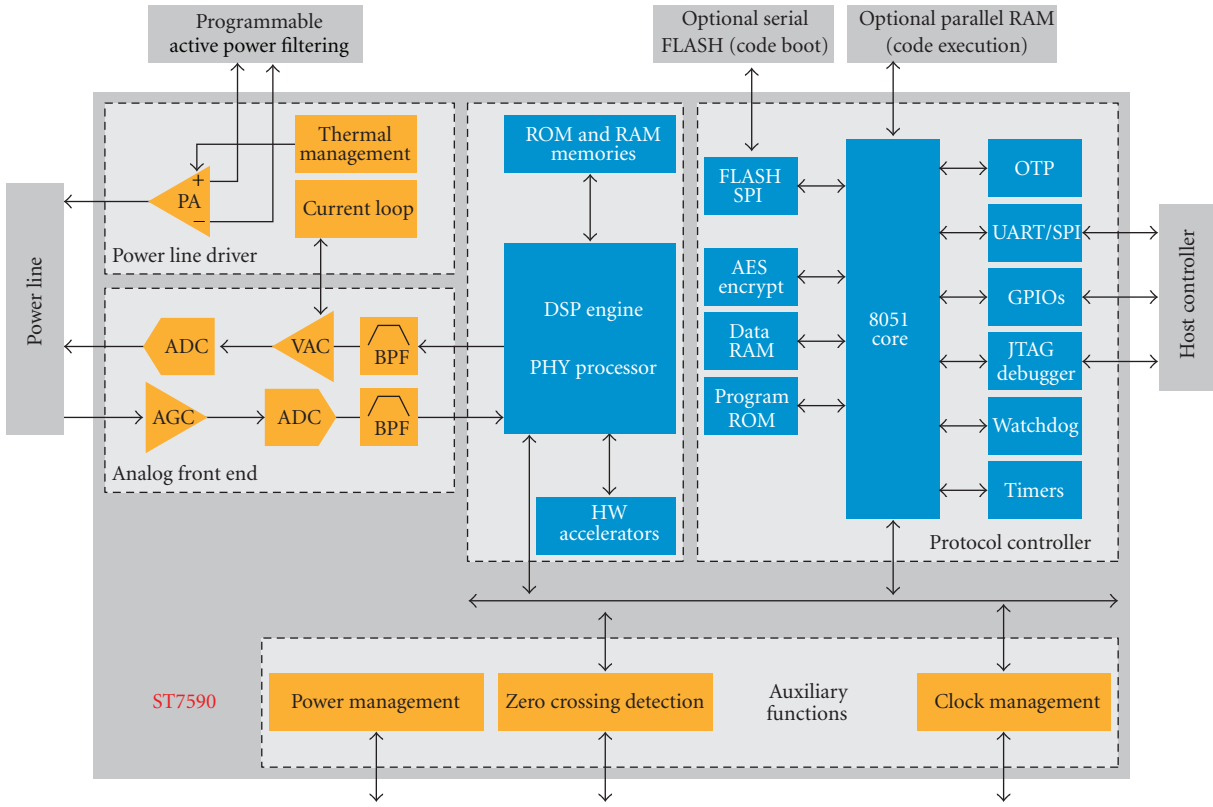


Figure 13: Architecture of the ST7590 PLC modem [25].

(i) *Extra encryption service*: the application and network layers use 128-bit AES encryption.

(ii) *Association and authentication*: only trusted nodes can join the network.

(iii) *Routing protocol*: the Ad hoc On-Demand Distance Vector (AODV) routing protocol specifies how nodes communicate with each other.

(iv) *Application service*: ZigBee introduces the concept of "cluster." Each node belongs to a cluster and can perform only actions allowed for the cluster. For example "house light system" cluster has only two possible actions: "turn lights on" and "turn lights off."

ZigBee nodes have a 16-bit network address, assigned by the coordinator during the association process. This address is used for routing information. Nodes within the network play different roles: coordinator, router, and end device. Coordinator and routers cannot sleep. They must be always awake in order to manage the network and to send packets along the network.

It is important to remind that the ZigBee network has not a peer-to-peer architecture, but a hierarchy one in which end devices can only communicate with routers and coordinators.

IEEE 802.15.4 supports only the encryption algorithm 128-bit AES. The reason is mainly due to the possibility to easily find on the market specific devices able to carry out encryption and decryption at the hardware level. The selected SoC has the AES processor embedded directly into transceivers and requires low resources. This standard does not specify how the keys have to be managed or the authentication policies to be applied. These details are leaved to the high-level standards. AES is used for data security (payload encryption) and for data integrity. In particular, the integrity is achieved using Message Integrity Code (MIC). MIC is obtained encrypting part of the MAC (Medium Access Control) frame, using the network key, and its length is usually 128 bits.

Figure 16 shows the IEEE 802.15.4 MAC frame. There are three important fields for security issues: frame control, auxiliary security header, and data payload.

Auxiliary security header field is meaningless if the security enable bit (within the frame control field) is unset. Otherwise, this field is divided into three subfields described hereafter.

Security Control. This field is used to select what kind of protection is used for the frame (i.e., security policies adopted): what is encrypted and how long is the key. The first 3 bits specify the security level, and related codes are listed in Table 5.

Frame Counter. To prevent replying attacks, every frame has an unique id.

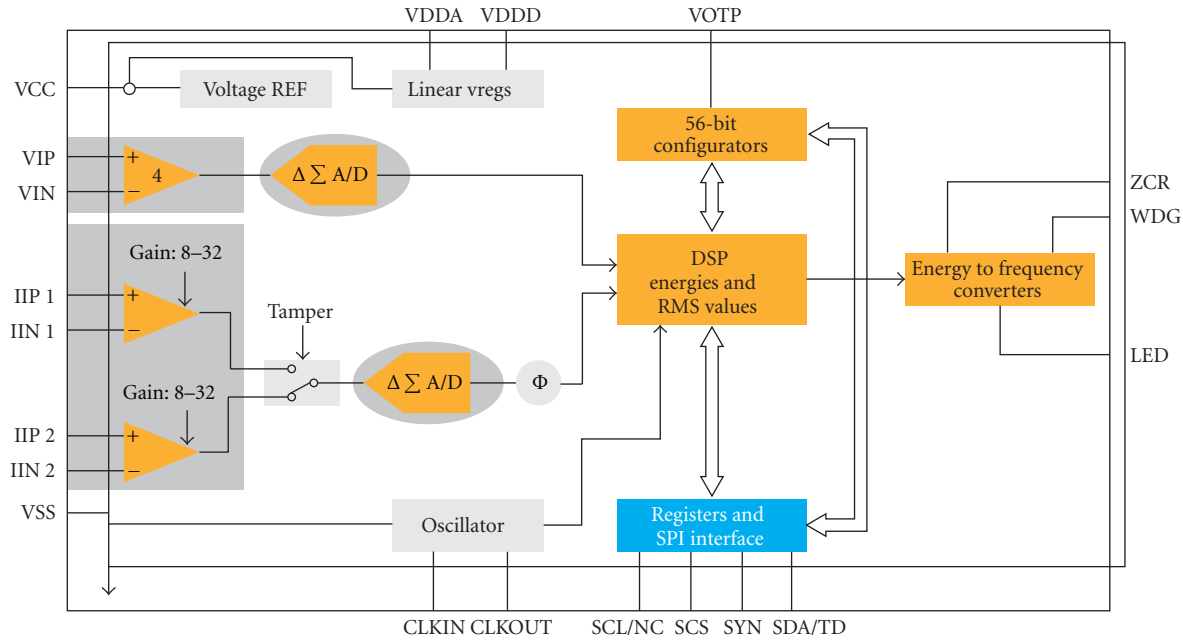


Figure 14: Architecture of the E-meter ASIC [25].

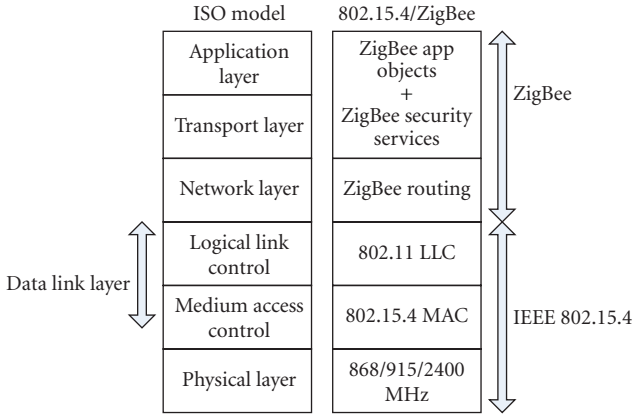


Figure 15: IEEE 802.15.4 and ZigBee role in the ISO/OSI stack.

Table 5: Security control codes.

Code	Security type	Authentication	Security services
0x00	No security	—	No security
0x01	AES-CBC-MAC-32	MIC-32	Data integrity
0x02	AES-CBC-MAC-64	MIC-64	
0x03	AES-CBC-MAC-128	MIC-128	
0x04	AES-CTR	—	Data security
0x05	AES-CCM-32	AES-CCM-32	Data integrity and security
0x06	AES-CCM-64	AES-CCM-64	
0x07	AES-CCM-128	AES-CCM-128	

Key Identifier. This field contains information about the type of key used in the communication with the other node. Keys can be implicit (known by nodes that are communicating) or explicit. In this last case, key index and key source subfields give indication about the key used.

Table 6: Access control list fields.

Field	Description
Address	Address of the destination node
Security suite	Security policy used
Key	128-bit key used in AES algorithm
Last initial vector (IV)	Used by the source to avoid reply attacks
Replay counter	Replay counter is equal to IV but is used by the destination node

Payload fields change according to security control field bits.

Every node within the network has an access control list (ACL), a list of "trusted brothers." Each node before sending data to another node checks if the receiver is a trusted brother using ACL table. If the receiver does not appear into the list, the node can take two possible actions, according to the security policy adopted for the network, reject the message or begin an authentication process. ACL fields are specified in Table 6.

With respect to the 802.15.4 layers, ZigBee adds two additional security layers: the network and the application layers. As all security mechanisms use 128-bit AES encryption, devices designed for IEEE 802.15.4 standard can be used without any modification. ZigBee standard uses three type of keys. These keys are actually used or not, according to the policy chosen for the network. ZigBee keys are:

(i) Master key: it is used for keeping link keys confidential and checking their correspondence.

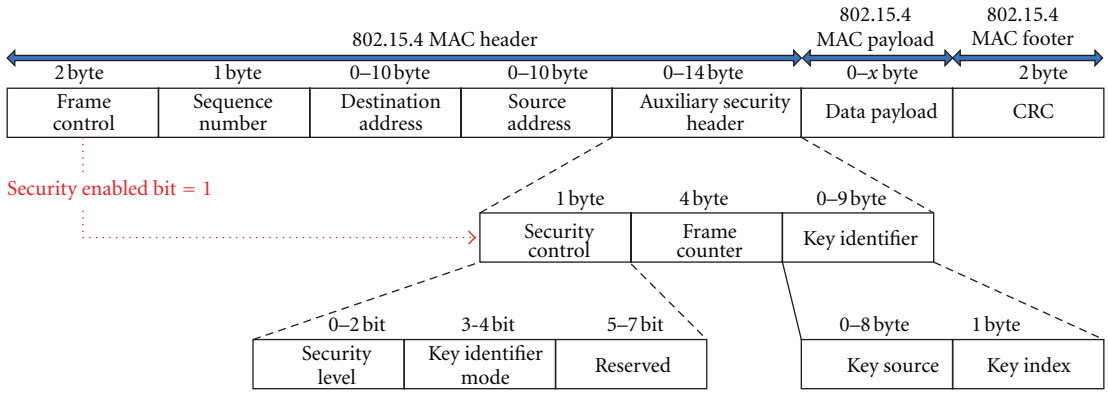


Figure 16: IEEE 802.15.4 MAC frame and security issues.

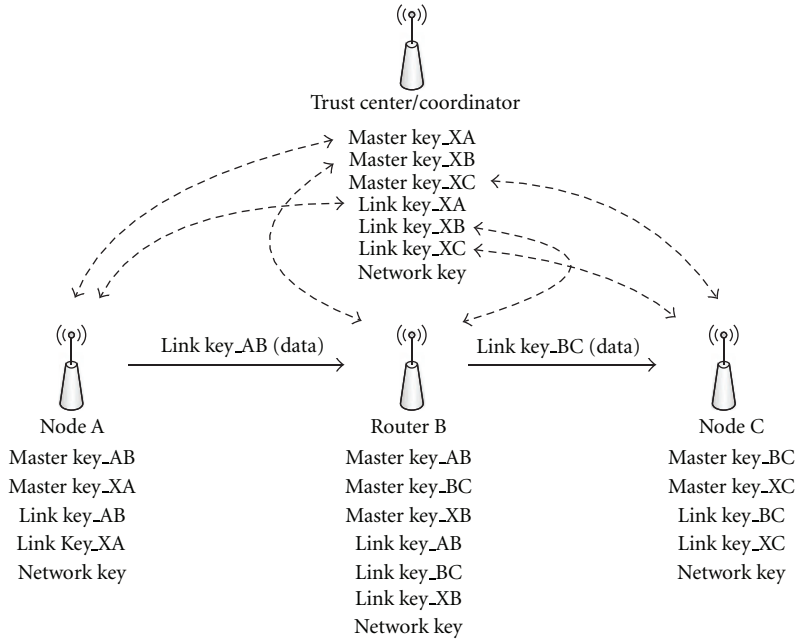


Figure 17: ZigBee commercial mode.

(ii) Link keys: these keys are unique between pair of nodes. The use of link keys introduces a significant overhead for the node, requesting more memory resources, due to the fact that all data exchanged between two nodes must be encrypted with this key. Link keys are used only in commercial mode policy.

(iii) Network key: it is an unique 128-bit key shared between the devices composing the network. Network key is generated by the trust center, and it is regenerated after specific time interval. The old key is used to encrypt the new key, that is sent to nodes.

Master and link keys are used by the application layer, and network key is used both by the ZigBee and the MAC layers. The trust center is a special device, that is trusted by the other nodes within the network. Generally, the coordinator is the trust center, even if this role can be played also by another node.

To ensure security, the ZigBee network can use both master and link keys, or if a simple connection is needed only the network key.

In the first case, ideally, every device has the trust center address and an initial master key preinstalled. Otherwise, master keys can be distributed by trust center, during initial network setup using an insecure channel. After all nodes have the master key, link key can be obtained using agreement or transport process. Link keys can be also preinstalled. An example of this use of keys is the commercial mode policy (shown in Figure 17).

When the ZigBee network uses only the network key there is an initial distribution of this key, that is done by the trust center through an insecure channel. Only after the network key is acquired by all nodes the communications between nodes become secure.

Security policies decide which keys are used to make safe the network.

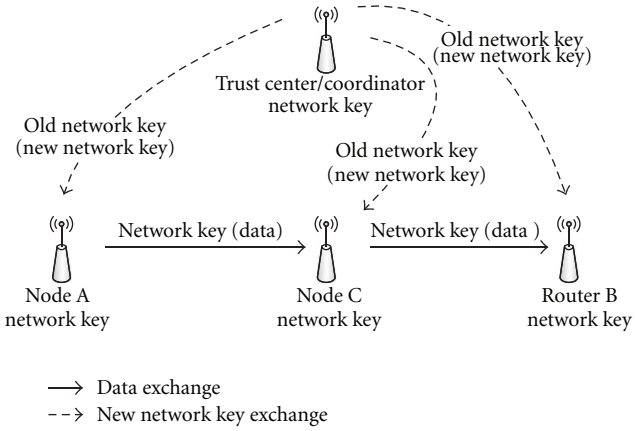


Figure 18: ZigBee residential mode.

(i) Commercial mode where both master key and link keys are used. In this case more memory resources are required.

(ii) Residential mode where data exchange within the network are encrypted using only network key. This mode is the easiest to implement but is less secure.

To ensure security and privacy protection in the example energy HAN, both residential and commercial modes (see Figures 17 and 18) can be used. In both modes, the trust center role can be played by the smart information box, that is also the coordinator of the network. This eliminates the need of a special node performing only security operations. Security parameters can be easily set using the interfaces of the smart information box, and information about network behavior (logs) can be stored and later accessed. Moreover, the Home Energy Angel smart information box is also accessible remotely, so users can control security status of the network also outdoor, using an internet connection.

To implement the residential mode the network will need only a network key. The Home Energy Angel smart information box can establish a first key and then distribute it through an insecure connection to other nodes. Otherwise users and operators can "write" it into the devices' memory; this operation is more secure. Actually any key is transmitted through an insecure channel. Summarizing, if residential mode is chosen security problems can occur during the initial setup of the network.

Commercial mode provides stronger security than residential mode but requires more resources (memory and CPU time). Actually each connection between two nodes uses different keys, and if security is broken in one link, this will not affect the whole network. Also in this mode, the initial key setting is a critical point. A secure method is to assign to each node a first master key "manually." Then, this will be changed by the trust center using a secure connection. If a first master key is not assigned, this task must be done by the trust center using an insecure channel. A successful conclusion of the initial setup of the network assures the confidentiality and the integrity of the network.

Information exchanged between nodes is always encrypted, and message integrity can always be checked, if the highest security level (AES-CCM-128) was selected. This choice does not affect devices performance since ZigBee transceivers have dedicated AES processors for encryption and decryption.

4. Conclusions

This paper has discussed and reviewed security problems in Smart Grid taking care of developed architectures and lesson learned at University of Pisa in some projects on the theme of smart energy. An energy home area network, a key element of Smart Grid, is presented, dealing with its security and privacy aspects and showing some solutions to realize a wireless network, based on ZigBee. Implementation challenges from the hardware and software point of view and possible architectures and implementation using COTS components are proposed for key nodes of the smart energy HAN: smart power meters, smart plugs, and a Home Energy Angel information box essential for energy management/saving policy and for energy awareness.

References

[1] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 2010.

[2] S. M. Amin and B. F. Wollenberg, "Toward a smart grid," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, 2005.

[3] W. K. Park, C. S. Choi, I. W. Lee, and J. Jang, "Energy efficient multi-function home gateway in always-on home environment," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 1, pp. 106–111, 2010.

[4] M. Jahn, M. Jentsch, C. R. Prause, F. Pramudianto, A. Al-Akkad, and R. Reiners, "The energy aware smart home," in *Proceedings of the 5th International Conference on Future Information Technology (FutureTech '10)*, pp. 1–8, May 2010.

[5] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 53–59, 2011.

[6] D. Y. Nagesh, J. V. Krishna, and S. S. Tulasiram, "A real-time architecture for smart energy management," in *Proceedings of the Innovative Smart Grid Technologies Conference (ISGT '10)*, pp. 1–4, January 2010.

[7] P. Kulkarni, S. Gormus, Z. Fan, and B. Motz, "A mesh-radio-based solution for smart metering networks," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 86–95, 2012.

[8] E. Pallotti and F. Mangiatordi, "Smart grid cyber security requirements," in *Proceedings of the 10th International Conference on Environment and Electrical Engineering (EEEIC '11)*, pp. 1–4, May 2011.

[9] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[10] EPRI, *Report to NIST on Smart Grid Interoperability Standards Roadmap*, EPRI, Gaithersburg, Md, USA, 2010.

[11] R. H. Lasseter and P. Paigi, "Microgrid: a conceptual solution," in *Proceedings of the IEEE 35th Annual Power Electronics Specialists Conference (PESC '04)*, pp. 4285–4290, June 2004.

[12] NanoCatGeo, "NanoCatGeo project," https://sites.google.com/site/nanocatgeo.

[13] Acta, "Hydrogen generators and fuel cells systems," http://www.actagroup.it.

[14] L. Fanucci, S. Saponara, and A. Morello, "Power optimization of an 8051-compliant IP microcontroller," *IEICE Transactions on Electronics C*, vol. E88, no. 4, pp. 597–600, 2005.

[15] S. Saponara, E. Petri, L. Fanucci, and P. Terreni, "Sensor modeling, low-complexity fusion algorithms, and mixed-signal IC prototyping for gas measures in low-emission vehicles," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 2, pp. 372–384, 2011.

[16] E. L. Quinn, *Privacy and the New Energy Infrastructure*, Social Science Research Network (SSRN), 2009.

[17] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*, Syngress, 2010.

[18] ZigBee, *The ZigBee Specification Version 1. 0*, ZigBee Alliance, San Ramon, Calof, USA, 2007.

[19] M. Zeifman and K. Roth, "Nonintrusive appliance load monitoring: review and outlook," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 1, pp. 76–84, 2011.

[20] T. S. Choi, K. R. Ko, S. C. Park, Y. S. Jang, Y. T. Yoon, and S. K. Im, "Analysis of energy savings using smart metering system and IHD (in-home display)," in *Proceedings of the Transmission and Distribution Conference and Exposition: Asia and Pacific*, pp. 1–4, October 2009.

[21] Z. Wang and G. Zheng, "Residential appliances identification and monitoring by a nonintrusive method," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 80–92, 2012.

[22] M. Venables, "Smart meters make smart consumers," *Engineering and Technology*, vol. 2, no. 4, p. 23, 2007.

[23] F. Benzi, N. Anglani, E. Bassi, and L. Frosini, "Electricity smart meters interfacing the households," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 10, pp. 4487–4494, 2011.

[24] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm '10)*, pp. 238–243, October 2010.

[25] Y. Gourdou, *Smart Grid/Metering Solution*, EMCU, 2011.

[26] M. Nassar, J. Lin, Y. Mortazavi, A. Dabak, I. H. Kim, and B. L. Evans, "Local utility power line communications in the 3–500 kHz band: channel impairments, noise, and standards," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 116–127, 2012.

[27] Echelon, *DCN, 1000 Series Data Concentrator*, Echelon, Memphis, Tenn, USA, 2012.

[28] IEEE, "IEEE guide for smart grid interoperability of energy technology and information technology operation with the Electric Power System (EPS), end-use applications, and loads," Tech. Rep. 2030-2011, IEEE, 2011.

[29] M. Weiss, A. Helfenstein, F. Mattern, and T. Staake, "Leveraging smart meter data to recognize home appliances," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom '12)*, pp. 190–197, 2012.

[30] ISO/IEC, *ISO/IEC, 27000:2009. Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*, ISO/IEC, Geneva, Switzerland, 2009.

[31] ISO/IEC, *ISO/IEC, 27001:2005. Information Technology—Security Techniques—Information Security Management Systems—Requirements*, ISO/IEC, Geneva, Switzerland, 2005.

[32] ISO/IEC, *ISO/IEC, 27002:2005. Information Technology—Security Techniques—Code of Practice for Information Security Management*, ISO/IEC, Geneva, Switzerland, 2005.

[33] ISF, *Information Security Forum's Standard of Good Practice*, ISF.

[34] K. Kent and M. Souppaya, "Guide to computer security log management," Tech. Rep. 800-92, NIST Special Publication, 2006.

[35] IEC/TS, "IEC/TS, 62351. Power systems management and associated information exchange—data and communications security," IEC/TS.

[36] A. Lee and T. Brewer, "Smart grid cyber security strategy and requirements," NISTIR Draft 7628, 2009.

[37] F. Hao and P. Y. A. Ryan, "Password authenticated key exchange by juggling," in *Proceedings of the 16th International conference on Security protocols*, pp. 159–171, Springer, Berlin, Germany, 2008.

[38] F. Hao and P. Ryan, "J-PAKE: authenticated key exchange without PKI," in *Transactions on Computational Science XI*, M. Gavrilova, C. Tan, and E. Moreno, Eds., pp. 192–206, Springer, Berlin, Germany, 2010.

[39] M. Blaze, "Protocol failure in the escrowed encryption standard," in *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, pp. 59–67, ACM, Fairfax, Va, USA, November 1994.

[40] C. Borean, "Energy@home: a "user-centric" energy management system," in *Proceedings of the 5th European ZigBee Developers' Conference*, Munich, Germany, 2011.

[41] N. Costantino, R. Serventi, F. Tinfena et al., "Design and test of an HV-CMOS intelligent power switch with integrated protections and self-diagnostic for harsh automotive applications," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 7, pp. 2715–2727, 2011.

[42] T. Jakobi and T. Schwartz, "Putting the user in charge: end user development for eco-feedback technologies," in *Proceedings of the 2nd IFIP Conference on Sustainable Internet & ICT for Sustainability (SustainIT '12)*, Pisa, Italy, October 2012.

[43] N. Goddard, J. Moore, C. Sutton, J. Webb, and H. Lovell, "Machine learning and multimedia content generation for energy demand reduction," in *Proceedings of the 2nd IFIP Conference on Sustainable Internet & ICT for Sustainability (SustainIT '12)*, Pisa, Italy, October 2012.

[44] F. Bellifemine, "Smart consumption: the energy@home approach," in *Proceedings of the 2nd IFIP Conference on Sustainable Internet & ICT for Sustainability (SustainIT '12)*, Pisa, Italy, October 2012.

[45] S. Genovesi, S. Saponara, and A. Monorchio, "Parametric design of compact dual-frequency antennas for wireless sensor networks," *IEEE Transactions on Antennas and Propagation*, vol. 59, no. 7, pp. 2619–2627, 2011.

[46] S. Genovesi, S. Saponara, and A. Monorchio, "Compact Triple-Frequency Antenna for Sub-GHz Wireless Communications," *IEEE Antennas and Wireless Propagation Letters*, vol. 11, pp. 14–17, 2012.

[47] A. G. Ruzzelli, C. Nicolas, A. Schoofs, and G. M. P. O'Hare, "Real-time recognition and profiling of appliances through a single electricity sensor," in *Proceedings of the 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '10)*, pp. 1–9, June 2010.

[48] A. Marchiori, D. Hakkarinen, Q. Han, and L. Earle, "Circuit-level load monitoring for household energy management," *IEEE Pervasive Computing*, vol. 10, no. 1, pp. 40–48, 2011.

[49] Freescale, *Electronic Tamper Detection Smart Meter Reference Design*, Freescale, 2012.

[50] J. McCullough, *Deterrent and Detection of Smart Grid Meter Tampering and Theft of Electricity, Water, or Gas*, Elster, 2010.

[51] ZigBee, *ZigBee and Wireless Radio Frequency Coexistence*, ZigBee Alliance, San Ramon, Calof, USA, 2007.

[52] G. Anastasi, M. Conti, and M. di Francesco, "A comprehensive analysis of the MAC unreliability problem in IEEE 802.15.4 wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 1, pp. 52–65, 2011.

[53] C. Gomez and J. Paradells, "Wireless home automation networks: a survey of architectures and technologies," *IEEE Communications Magazine*, vol. 48, no. 6, pp. 92–101, 2010.

[54] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," in *Computer Networks*, vol. 38, pp. 393–422, Elsevier, New York, NY, USA, 2002.

[55] D. M. Han and J. H. Lim, "Smart home energy management system using IEEE 802.15.4 and zigbee," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1403–1410, 2010.

[56] Atmel, *ZigBit 2.4 GHz Wireless Modules—ATZB-24-A2/B0*, Atmel, 2009.

Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2012, Article ID 190639, 15 pages
doi:10.1155/2012/190639

Research Article

Experimental Evaluation of a SIP-Based Home Gateway with Multiple Wireless Interfaces for Domotics Systems

Rosario G. Garroppo, Loris Gazzarrini, Stefano Giordano, and Luca Tavanti

Dipartimento di Ingegneria dell'Informazione, Università di Pisa, 56126 Pisa, Italy

Correspondence should be addressed to Luca Tavanti, luca.tavanti@iet.unipi.it

Received 28 July 2012; Revised 9 October 2012; Accepted 9 October 2012

Academic Editor: Gildas Avoine

In modern houses, the presence of sensors and actuators is increasing, while *communication services* and *entertainment systems* had long since settled into everyday life. The utilization of wireless communication technologies, such as ZigBee, Wi-Fi, and Bluetooth, is attractive because of their short installation times and low costs. The research is moving towards the integration of the various home appliances and devices into a single domotics system, able to exploit the cooperation among the diverse subsystems and offer the end-user a single multiservice platform. In this scenario, the paper presents the experimental evaluation of a domotics framework centered on a SIP-based home gateway (SHG). While SIP is used to build a common control plane, the SHG is in charge of translating the user commands from and to the specific domotics languages. The analysis has been devoted to assess both the performance of the SHG software framework and the negative effects produced by the simultaneous interference among the three widespread wireless technologies.

1. Introduction

Domotics refers to a system that controls several (or all) home "services," such as lighting, HVAC (heating, ventilation, and air conditioning), communications, security, healthcare, and entertainment, in a integrated and automatic or semi-automatic way, allowing the user to manage them from a series of heterogeneous devices (e.g., touch panels, remotes, mobile handsets, and smartphones), either at home or from anywhere in the world. In the domotics archetype, all subsystems are able to talk to each other and interact in a seamless manner, realizing an intelligent structure that improves the quality of life, reduces the costs, and achieves energy savings. To put this paradigm into practice, the communication among the single devices and between the various subsystems is the fundamental operation. Hence, wired and wireless networks will be one of the building blocks of the present and future domotics solutions. On top of this somewhat "physical" element, a common control plane is also necessary, in order to unify the management operations into a single and portable user interface.

One of the major components of a domotics system is the set of sensors and actuators. These usually come in the form of one or more networks, backed either by a single technology or by different ones. Not always, however, do the specifications define a common control plane that is suitable to contemporarily manage devices belonging not only to different standards, but even to different application profiles. As a result, the burden of coordinating and making devices interoperate is often left entirely to the system implementer. Indeed, a scenario with mixed profiles and technologies is not so uncommon, especially in those environments where multiple services might be requested. One such example is exactly the "smart home" or domotics concept, in which several profiles and technologies (e.g., ZigBee's home automation, smart energy, and telecom services, or KNX's lighting, heating, and energy management—just to cite the most appealing ones) might all be present.

From the user perspective, the devices belonging to the diverse subsystems of the home services platform can be typically controlled through dedicated appliances located in the house (e.g., a touch panel, a smart telephone, a TV

remote). However, this paradigm no longer holds for remote control operations that occur when the user is far from home. In this case the user would normally have a single device at hand, such as a notebook or a smartphone, by means of which he/she would like to control any device in the home, not just those belonging to a specific profile or technology, and possibly without complex configuration or selection procedures.

In addition to the need for a coordinating system for the DSANs, in today's houses we already find interpersonal communication and multimedia entertainment systems. Hence, the design of a domotics platform should also consider the integration of communication and multimedia applications with the DSAN-based services.

In this scenario, we describe an architecture designed to gain interoperability among devices belonging to different technologies and profiles. In our vision, the common control plane is realized through the Session Initiation Protocol (SIP) [1], while a *SIP-based home gateway* (SHG) translates the user commands from and to the specific DSAN language, thus allowing the user to control all domotics devices either at home or away from it, using his mobile terminal or his favorite SIP client, in a transparent, uniform, and simple way. The SHG, which is the major enabler of the envisioned system, is also devised to retain the compatibility with the existing SIP infrastructure and the deployed SIP clients, which can therefore be exploited in full.

Among the various domotics sensor and actuator networks (DSANs), wireless sensor networks (WSNs—note that the term "sensor" is often used for both sensors in the strict sense and for actuators too) are the version that is growing faster, due to shorter deploying times and simplified configuration. Several technologies and standards are nowadays available for the implementation of a WSN [2]. Especially the ones based on open or widely adopted standards, such as ZigBee, Bluetooth, *Z*-Wave, and KNX-RF, can undeniably be regarded as the most interesting ones. This is because they allow the deployment of large and almost self-configuring networks in relatively short times and at reduced costs. Two of these standards, ZigBee and Bluetooth, have been embedded into the SHG.

On the other hand, the current trend in multimedia and communication home systems is to move the physical transport services over the Wi-Fi technology. Thus, we have equipped our SHG also with a Wi-Fi interface, used for providing the above-mentioned "wideband" services.

The majority of these wireless standards operate into the unlicensed 2.4 GHz ISM band, which can be exploited by multiple users and networks at the same time. However, due to the mutual interference, the coexistence of different devices operating in proximity of each other can be troublesome. As proved by many authors [3, 4], this is especially true for ZigBee networks, whose performance is heavily influenced by the presence of Wi-Fi devices. While it is sometimes feasible to avoid the interference among devices sharing the same spectrum and implementing the same standard (e.g., collision avoidance schemes might work across separate networks), the use of incompatible modulations and channel access schemes makes it virtually impossible to ensure the coexistence among devices belonging to different technologies.

In summary, the design and implementation of a domotics gateway must face two key issues: integrating heterogeneous indoor devices and networks, allowing the composition of dynamic and pervasive services (including interpersonal communications and multimedia), and assuring the physical coexistence of the interfaces located on the gateway apparatus.

1.1. Contribution. We present a working prototype of the SHG, which is used to build a complete proof-of-concept of our SIP-based domotics architecture. A customized SIP event package and a notification server have also been developed to validate a possible extension to new services. The SHG was interfaced with an actual ZigBee network and a Bluetooth PAN, in addition to a generic Wi-Fi connection. We experimentally evaluated the performance of the SHG prototype, proving its ability to support large domotics systems.

In describing our SIP-based system, we also present the aspects that make it innovative. We arranged for the SHG to be the sole entity to have a SIP address, thus avoiding the overhead of having a SIP address for each home device. We designed and implemented a functional addressing and a control scheme to ease the user interaction with the system and an abstraction layer to decouple the implementations on the SIP and DSAN sides. We also show how we exploited some features of ZigBee to improve the integration with the SIP and the SHG.

Then, the paper reports an experimental study involving Wi-Fi, ZigBee, and Bluetooth networks. The goal of this study is to characterize the performance of the SHG in terms of the coexistence of the three systems, especially because they are all active in the same time and space, that is, in the prototype SHG board, and thus subject to strong mutual interference.

2. Related Work

In this section we just draw a sketch on the current state of the art in domotics systems and interference studies, with specific focus on the works whose topic is most similar to ours. The differences that make our contribution innovative are also pointed out.

Starting from the domotics area, some authors approached the integration between WSNs and control plane protocols by bringing customized or reduced versions of SIP or REST on the sensor nodes. For example, Luckenbach et al. [5] employed REST to provide clients connected to the Internet with the ability to directly interact with MICAz sensors. Similarly, Krishnamurthy and Lange [6, 7] proposed TinySIP, an architecture to offer to multiple clients the access to sensor-based information via SIP.

These kinds of approaches suffer from a series of drawbacks. Since the device is resource constrained, the protocols must be stripped of many functionalities. Due to the particular operative system running on the sensor nodes,

the development times might be nonnegligible. Also, given the high heterogeneity of the devices, it might be necessary to repeat and modify the customization and development steps for every technology that is going to be integrated into the system. Finally, compatibility with deployed hardware and software is not retained. Conversely, our framework moves the development effort to a single high-end device (the SHG), allowing faster implementation times and full compatibility with both existing sensor and actuator devices and also with the SIP.

An approach that follows the philosophy of making an open and flexible service platform can be found in [8], whose authors started their work from an architecture similar to ours.

Acker et al. [9] presented a concept of ubiquitous home and facility control that exploits the IP Multimedia Subsystem (IMS), a SIP-based control architecture considered by mobile network operators.

The work closest to ours is perhaps the one by Bertran et al. [10, 11], who tested SIP as a universal communication bus for home automation environments. A SIP gateway and a series of SIP adapters and interpreters have been implemented and deployed to make all devices SIP compliant. However, there are some aspects that may put our framework one step ahead.

Bertran et al. did not consider the issues with addressing and reachability of the single DSAN devices. Conversely, we designed a functional addressing scheme that greatly simplifies the user interaction and does not require the DSAN nodes to register to any SIP server or other additional entities. Then, we devised a way of keeping the compatibility not only with the DSAN elements, but also with the user terminals. This allowed us to provide the user also with functionalities that are not natively supported by his/her device. This paradigm can even be extended to ensure forward compatibility with new domotics services. Conversely, Bertran et al. did not pay much attention to this aspect. A third distinguishing point is in the adaptation between the SIP and the DSAN worlds. While Bertran et al. design a single software module to be put in the gateway, we perform this operation in two steps, via the DFA layer. This allows to decouple the implementation of the two domains, making the system more flexible. Finally, we studied in much more detail the integration with two possible DSANs, namely, ZigBee and Bluetooth, and showed how it is possible to exploit their features to simplify the integration into the system. In [11], the main focus of the experimental platform was on the performance figures of the gateway (which, if we consider the current hardware technology, might not be the most relevant hurdle to the domotics development, as proved by our tests in Section 7.2).

A major disadvantage that is common to proposals like [8–10] is the need for every home device to register with its own URI. When the number of devices increases (heavily monitored and automated buildings may have hundreds of nodes), the user capability of handling them through their URIs is clearly hampered. The same shortcoming applies to the zone manager solution proposed by [6], in which the majority of the communications are possible only by knowing the address of each gateway to which the sensors of interest refer. On the other hand, in our system the sole SHG must register to an external SIP server (unless the SHG itself implements a registrar) and we can mask the multitude of DSAN nodes by means of the "functional addressing" method.

As for the coexistence of multiple wireless interfaces, we can find numerous analytical and simulation studies, especially about the performance of ZigBee under the interference of Wi-Fi and Bluetooth (such as [12], just to cite one). The major shortcoming of these approaches is that due to the very complex nature of the wireless channel and environment, there is no measure of their agreement with the reality, and thus their actual utility is somehow limited.

Sikora and Groza experimentally obtained the PER of a ZigBee system under the interference of Wi-Fi devices, Bluetooth devices, and also a microwave oven [4]. However, the study is limited to a single source of interference (e.g., either Wi-Fi or Bluetooth), and also the analysis of the coexistence of ZigBee and Bluetooth is not complete, since the (actually very few) results have been collected in one direction only (i.e., Bluetooth over ZigBee). Nevertheless, an interesting observation in Sikora and Groza's paper is about the presence of notable discrepancies between the collected experimental data and the simulation results provided by the IEEE 802.15.4 task group.

A similar experimental study was led by Musaloiu-Elefteri and Terzis, who evaluated the loss rate of a ZigBee system under Wi-Fi interference [3]. Starting from this result, they developed interference estimators and distributed algorithms to dynamically change the ZigBee operating channel. This approach was proved to drastically reduce the loss rate of ZigBee networks.

The authors of [13] present the results of an empirical study on the coexistence between IEEE 802.11b and Bluetooth devices. However, the primary objective was to develop an analytical model to estimate the mutual interference, rather than characterizing it in real world scenarios. Hence, to build such models, the experiments were controlled through the use of attenuators, signal generators, and coaxial cables, thus resulting in a rather idealistic environment.

From the analysis of the cited works, it emerges that in all cases, even in [4], the authors studied the interference of no more than two systems at a time. A two-way experimental analysis of the simultaneous interference among Wi-Fi, Bluetooth, and ZigBee can be found in [14], which confirms the weakness of ZigBee and also shows that some supposed interference-free ZigBee channels are in fact affected by the presence of Wi-Fi transmissions.

However, in all cited works, the interfering sources are always placed in physically disjoined devices. On the contrary, devices such as the domotics gateways are expected to embed several wireless interfaces onto the same board. In such cases, the interference effect might be even greater, due to the electrical couplings on the board. The experimental measurement we carried out over our prototype SHG was aimed at filling this gap.

3. Domotics Requirements and the SIP Control Plane

The complexity of the domotics system demands for a series of requirements that allows an easy integration among the subsystems and the development of a "friendly" and always available user interface. A set of the major requirements is represented by the following list (see also [8, 15] for similar surveys).

(i) The domotics system must implement and provide a *request/response* paradigm to allow the user to send commands to the DSAN devices and possibly have a feedback. Commands can also be exchanged among the various domotics entities.

(ii) Both the user and the system should be promptly notified when events of some importance occur in the environment. Thus, the network is expected to support asynchronous and/or periodic *event notification*.

(iii) Commands and events suit the need of exchanging small amounts of data in very short times. The use of *sessions* would instead allow the streaming of various types of data over a period of time (e.g., audio and video, but also fast varying sensor readings or large file transferrals).

(iv) The extensive adoption of mobile devices such as smartphones and tablets has made the connection to the global network available everywhere. As a consequence, the user should be regarded as a *mobile user*, who would want to control his/her home from different places and via diverse access technologies (e.g., wireless LAN, cellular, ADSL).

(v) Despite the heterogeneity of the various domotics subsystems, the user would hardly be keen on using several and different human interface devices (HIDs), remembering the network addresses of every DSAN device, or learning technology-specific aspects of its domotics system. Conversely, it would be beneficial if the user could interact with a unique interface layer and associate mnemonic names to the devices and their functions (i.e., what we later call "functional addresses", e.g., the room where they are placed and/or the action they perform). Therefore, the domotics system should *integrate the subsystems* at both the technical and the user interface level.

(vi) While the domotics idea is slowly gaining field, *communication services* and *entertainment systems* had long since settled into everyday life. Therefore, the design should seamlessly include these services into the domotics platform (see [10] for some interesting examples).

Among the many options for realizing the common control plane (see, e.g., [15–19]), we selected the Session Initiation Protocol for its numerous advantages. From the conceptual point of view, which relates to the operations that are to be carried out by the control plane, SIP provides a set of *methods* that fit well the necessities of DSAN control and management as follows.

(i) The low overhead of the `MESSAGE` method (no set-up phase is needed) perfectly matches the requirements of the *request/response* operations.

(ii) A publish/subscribe-notify semantic is available in SIP specifications and allows the user to be promptly notified of events that occur in the network. This allows an almost direct mapping of asynchronous and/or periodic *event notifications* to SIP methods.

(iii) SIP has been natively designed to offer *session management* capabilities (i.e., session creation, modification, and tear down).

(iv) The core SIP infrastructure exploits the `REGISTER` method to transparently manage the movement of the user between different points of attachment to the network.

From a more practical and implementation perspective, we can identify the following key points.

(i) SIP is a text-based protocol: message building and parsing is a relatively simple task. SIP parsers and interpreters are widely available. Hence, the development effort is greatly reduced.

(ii) The body of SIP messages is flexibly structured and can contain a wide variety of information. This allows an easy extension of the protocol to support customized DSAN-related data and commands.

(iii) A huge SIP infrastructure is already deployed and working; hence, there is no need to deploy new infrastructural elements (either servers or core-network software).

(iv) SIP works at the application layer, being transparent to the underlying physical and networking technologies. It can thus work as a gluing layer for heterogeneous systems.

A further valuable asset of SIP is the use of *mnemonic names*. Every SIP resource is associated to a URI (uniform resource identifier), a mnemonic text pattern based on the same syntax established for web services. This allows the user to remember names rather than complex numeric addresses. A way of exploiting this feature is presented later on in the paper.

Despite its numerous advantages, employing SIP for the control plane of our domotics system does not come for free. There are several issues that must be solved as follows.

(i) SIP is defined by a series of RFCs that provide only general indications on the use of the standardized procedures. The application to practical cases is left to the implementer, and it clearly depends on the specific scenario. Hence, the usage of SIP might require a preliminary phase to map the existing methods and design complementary procedures that fit the application requirements. One such example

is the Event Notification Framework, a standardized but empty framework in which we have defined a new package to be used in our domotics architecture (see Section 6.3).

(ii) To be effective, a control plane must be pervasive and its procedures supported by all devices forming the system. However, porting SIP on devices with minimal processing and/or storage capabilities, such as the sensors and actuators, is a nontrivial task that is often reduced to porting just a subset of the original methods and features (see, e.g., [6]). Clearly, this approach is not optimal and should be avoided in favor of a complete transposition of the available paradigms and/or capabilities.

(iii) Though SIP is a mature and relatively widespread technology, the majority of end-user devices employ SIP to support very few services. Designing a system under the assumption that all user devices can support all SIP methods is undoubtedly appealing, but quite unrealistic as well. Conversely, defining the procedures to allow the users to take advantage of these paradigms by means of their current terminals is a harder but definitely more sensible task.

3.1. Selected SIP Methods. In this subsection we provide a brief description of the SIP methods we used and how we integrated them into the domotics system. Note that the integration mode is not univocal and other mappings can be implemented. Therefore, particular attention is paid to the reasons that drove our choice, how these methods have been exploited, and how they interact with the other elements of the system.

3.1.1. Instant Messaging. The SIP `MESSAGE` method [20] is used to supply the real-time dispatch of short text messages where each message is independent from the others. A `MESSAGE` transaction requires no session setup and does not establish a dialog. The UA receiving a `MESSAGE` must send an immediate reply to the sender to inform it about the successful or failed reception of the message—in case of success, the answer is `200 OK`.

We used this real-time and low-overhead method to implement the *request/response* paradigm (see Section 3). In detail, the *request* is mapped to a first `MESSAGE` transaction, and the *response* is mapped to a second `MESSAGE` transaction. Therefore, four SIP messages are necessary to realize the *request/response* paradigm. A typical usage case of this method is illustrated in Figure 1.

A very important aspect of the `MESSAGE` method is its compatibility with all existing SIP clients. Since every SIP client must support this method, this ensures that the basic managing functions of our system are also supported.

3.1.2. Publish/Subscribe-Notify Paradigm. The SIP Event Notification Framework (ENF), defined in [21], provides a way for SIP elements to learn when "something interesting" has happened somewhere in the network. The procedures to allow for the prompt distribution of such events are known as the Publish/Subscribe-Notify paradigm.

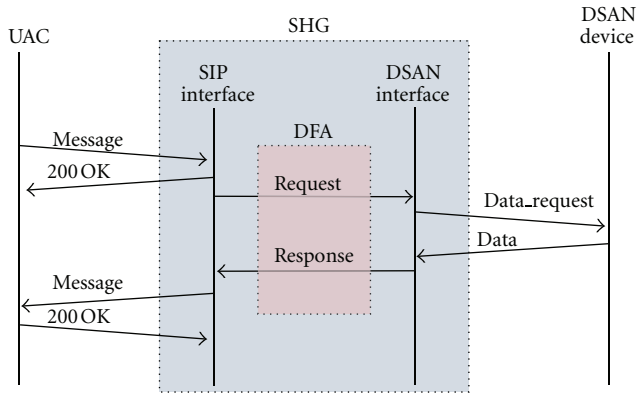


Figure 1: The *request/response* paradigm implemented via the `MESSAGE` method.

Briefly, an initial `SUBSCRIBE` message is sent by the subscriber (the user that is interested in the event) to the notifier (the node that is first aware of the event). If the subscription is accepted, a `200 OK` answer is sent to the subscriber. Then, the events are reported from the notifier to the subscriber by means of the `NOTIFY` method. Notifications can be sent either periodically or when the specific event occurs (or both).

SIP also provides a framework for the publication of event states on a notification server, called Event State Compositor (ESC). This task is accomplished using the `PUBLISH` method [22]. The ESC is then responsible for managing and distributing this information to the interested parties through the ENF.

The mapping of the complete Publish/Subscribe-Notify paradigm to the domotics architecture is shown in Figure 2. The figure shows both periodical and event-driven notifications.

Note that the ESC is a logical entity, which can physically reside in diverse parts of the system; in our prototype the ESC functions are provided by the SHG. In particular, the SHG is the only entity that publishes the events. DSAN devices are thus preserved from knowing anything about the SIP existence. In addition, the SHG can filter and compose events that are not available in the single DSAN domains.

3.1.3. Registration. In the proposed domotics architecture, just two elements must be registered: the user and the SHG. All sensors and actuators of the various subsystems are managed by the SHG via the specific DSAN interfaces. Thus they can be completely unaware of the SIP control plane. On the other side, the user can interact with the system by knowing just the SIP URI of the SHG and can refer to the DSAN devices through what we have called the "functional addressing" scheme (see Section 4.2), that is, a set of mnemonic names (such as the room names and the device functions). This makes the system extremely user-friendly and also highly scalable. No matter how many devices are in the house, the user can control them invariably

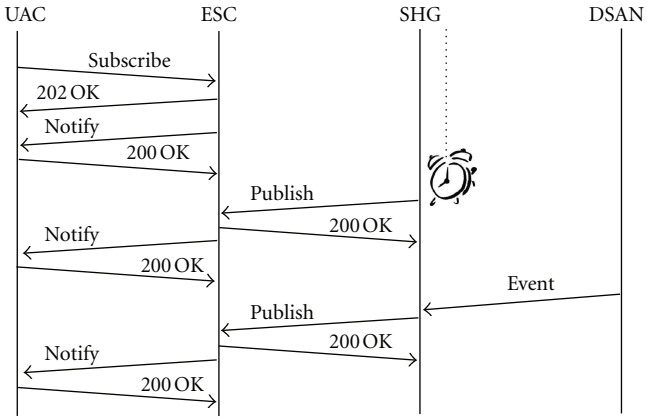


Figure 2: SIP message flow for publish, subscribe, and notify operations over the domotics system.

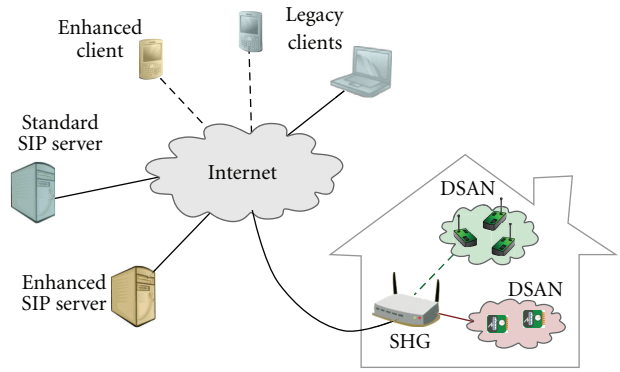


Figure 3: Reference architecture of the SIP-based domotics system.

through the same URI (the SHG one), from anywhere he/she is and from any SIP-enabled device he/she is using.

4. System Architecture

The general architecture of the conceived domotics system is illustrated in Figure 3. We can identify four major physical elements: the clients, the SIP servers, the SHG, and the DSANs.

The expert reader may have noticed that this kind of architecture is not completely novel: a similar picture has been presented, for example, by [8, 10]. This means that the scenario in which the domotics system is going to operate can be considered quite settled. Nevertheless, though addressing a similar architecture, the various works, and ours in particular, differ in several aspects, such as how the SIP is integrated into the framework and exploited by the designer, what semantics are taken into account, how they interact with the other components of the system, and how they can be beneficial to the user. Specifically, our approach targets a more scalable, transparent, and painless integration, both from the user perspective and from the DSANs' point of view.

The new and distinguishing elements of the architecture are described in the following.

4.1. SIP-Based Home Gateway. The SIP-based home gateway (SHG) is the key element of the system. It enables the remote control of the various DSANs by translating the messages and procedures from the SIP world to the specific DSAN technology and vice versa. Furthermore, it performs "intelligent" operations, such as piloting devices of a DSAN in response to events from another DSAN (e.g., turn on a KNX-enabled heater after a ZigBee sensor has reported a temperature/humidity change) and interpreting generic user commands and mapping them to device-specific actions.

The complete description of the SHG prototype is reported in Section 6.1.

4.2. Domotics Facility Abstraction. An intermediate entity, named domotics facility abstraction (DFA), has been introduced with a double goal: disjoin the implementation of the two domains of the system (i.e., the SIP and the DSANs) and create a single and user-friendly service abstraction. The former goal is meant to ease the development of the SIP and the DSAN interfaces, which may be carried on separately. The abstract definition of the domotics services enables the *functional addressing and control* paradigm employed for the user interface, leaving SIP on the pure transport layer, which is thus hidden to the user.

A pictorial description of the framework can be seen in Figure 4. The user is immersed into the functional service abstraction, which is implemented through the user interface on the client, and is understood and processed at the SHG. As it will be detailed in Section 6.1, the DFA is realized for the most part in the SHG, which stores the set of actions and performs the necessary tasks to accomplish the user's directives.

An example application of this framework can be swiftly provided. Imagine a user at a remote place (e.g., returning from a travel abroad) wishing to find the home at a comfortable temperature. He/she can then issue a simple command, such as "set home temperature 20." The client then wraps the command into the proper SIP procedure and conveys it to the SHG, where it is mapped to a DFA service. The SHG then cares for translating it into a proper set of DSAN operations, such as starting the HVAC system and setting an alarm threshold on the temperature sensors deployed in the house. When the desired temperature is reached, the SHG will automatically stop the HVAC system.

We can see from this example that the user demands a specific operation to be performed, but he/she is clearly ignoring all the technical processes of the domotics system, which are transparently handled by the SHG by means of the DFA layer.

4.2.1. System Configuration and Reconfiguration. Clearly, to unleash the capabilities of the DFA layer and the functional addressing and control scheme, a configuration phase must take place. In our vision, this phase can be split into two steps.

In the first step, occurring during the system development, the set of actions and user keywords must be defined and implemented. With reference to the previous example, the developer should make the SHG aware of the keywords "set," "home," and "temperature" and implement

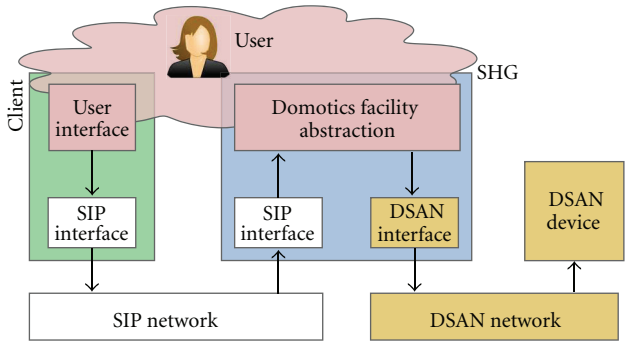


Figure 4: The functional paradigm implemented via the domotics facility abstraction.

the procedures that transform these keywords into real actions (such as sending a command to a HVAC actuator). Yet, these procedures cannot address a specific device, since the set of available devices will only be known at deployment time. Therefore the procedures can define just generic commands that become actual technology-specific actions once the DSAN devices are connected. For example, typical general HVAC actions could be "heat," "ventilate," and "cool." The completion of this phase defines the set of keywords and paradigms the user can take advantage of.

The second configuration step takes place at deployment time. Having a look at Figure 7, which shows the SHG internals, might help making the concept clearer. The installation-specific details, such as the plan of the house and the room names, are stored into the SHG database and/or file system. This task can be performed either by the installer or by the user. Offering a GUI to let the user install and/or configure the SHG might be a commercial choice. At the same time, the DSAN managers detect the connected devices and populate the SHG database, inserting information such as the device types, capabilities, and the actions they can perform. The physical position of the devices is inserted by the user/installer, after the devices have been registered with the SHG.

The system is now ready to work. When a user request is received, the SHG will map it to the appropriate action, search its database for the device(s) supporting that action, and issue the command(s) towards those DSAN devices. The full workflow of the SHG and its internals are described in Section 6.1.

Obviously, the information entered during the deployment phase can be modified later on, for example, as a consequence of device movement, replacement, or addition. Though being a more delicate operation, also the set of keywords and actions available to the user can be changed, for example, by upgrading the SHG firmware.

5. Wireless Technologies in the SHG

In this section we give a quick overview of the three wireless technologies, that is, Wi-Fi, ZigBee, and Bluetooth, that we have selected for the Home Network and hence, integrated onto the SHG prototype board. We also outline how these standards exploit the 2.4 GHz band and interact in this region of the spectrum.

5.1. Wi-Fi. The latest IEEE 802.11 standard [23] defines a CSMA/CA (carrier sense multiple access with collision avoidance) scheme as the mandatory medium access scheme. According to CSMA/CA, every Wi-Fi device shall listen to the medium before transmitting. The transmission is allowed only if the medium has been sensed idle for a predefined time period. In case the medium is sensed busy or after a collision, the device shall refrain from transmission for a period whose length is determined by a random variable (exponential backoff).

An IEEE 802.11 network can operate over one of the 11, 13, or 14 channels defined for the 2.4 GHz ISM band (the exact number depends on the local regulations). Each channel is 22 MHz wide, and the channels are partially overlapped (since the overall ISM bandwidth is just above 80 MHz). Therefore, no more than three networks can be contemporaneously operated in the same area in order to keep the transmissions of each free from interference from the others.

The operative channel and the transmission power are generally set statically (e.g., by the manufacturer or by the user at configuration time), even though dynamic channel selection (DCS) and transmit power control (TPC) routines have been defined for operations in the 5 GHz band. In the 2.4 GHz band, the maximum transmission power is 100 mW (20 dBm) in Europe and 1 W (30 dBm) in North America; in Japan, where power is measured in relation to bandwidth, the maximum allowed power is 10 mW/MHz.

Finally, the modulation scheme is either a DSSS (direct sequence spread spectrum) for the lower bit rates or an OFDM (orthogonal frequency division multiplexing) for the higher ones.

5.2. ZigBee. The IEEE 802.15.4 standard [24] specifies the physical and medium access control layers for low-rate wireless PANs, targeting a 10-meter communication range with a transfer rate of up to 250 kb/s.

Similar to Wi-Fi, 802.15.4 devices employ a CSMA/CA channel access algorithm and the DSSS modulation (actually, the latest release of the standard defines four modulation schemes, but in the 2.4 GHz band only the DSSS modulation is allowed).

Sixteen channels are defined for worldwide use in the 2.4 GHz band. However, differently from 802.11, they are much narrower (just 2 MHz) and do not overlap, so that up to sixteen 802.15.4 networks can easily coexist in the same area. When starting a new network, an energy detection (ED) functionality is used to determine the activity of other systems and thus decide the operating channel; yet there is no support for dynamic channel selection.

The latest ZigBee release has introduced the support for frequency hopping in the "ZigBee Pro" standard. In this way a PAN coordinator can move the whole PAN to another channel if the one in use is overloaded. However, this is not

a fast, reliable, and energy saving way to solve the problem. In addition it is not mandatory to implement.

5.3. Bluetooth. Bluetooth is a standard communication protocol designed for connection-oriented services such as voice, with low power consumption and short-range operations. The output power depend on the device class, spanning from 1 to 100 mW. Accordingly, the expected range should go from 1 to 100 meters, even though the practical range is highly variable.

Bluetooth transmits on up to 79 channels in the 2402–2480 MHz range. Each channel is 1 MHz wide, and one guard channel is used at the lower and upper band edges. In order to reduce the interference from external sources, frequency hopping (FHSS) is used to spread the signal across all channels. Thus a single Bluetooth network uses the full available 2.4 GHz ISM band. Different networks can coexist in the same area by employing different hopping patterns or a time-shifted version of the same pattern. Since Specification v1.2, Bluetooth also includes an adaptive frequency hopping (AFH) scheme, which reduces the number of employed channels to improve its robustness against the interference.

The Bluetooth channel access procedure is based on a master-slave scheme, which is built on the top of a time division duplex (TDD) transmission scheme. The basic modulation is Gaussian frequency-shift keying (GFSK), which allows a transfer rate of up to 1 Mb/s. Since the introduction of the enhanced data rate (EDR) with specification v2.0, $\pi/4$-DQPSK (differential quadrature phase shift keying) and 8-DPSK modulations may also be used, bringing the data rate to 2 and 3 Mb/s, respectively.

5.4. Channels, Frequencies, and Modulations. Figure 5 shows the allocation of the ZigBee and Wi-Fi channels over the 2.4 GHz ISM band. Note that a single 802.11 channel completely overlaps with four ZigBee channels. Bluetooth channels are not reported, as the FHSS covers the whole available spectrum.

The three most used nonoverlapping Wi-Fi channels are 1, 6, and 11. In this case, two ZigBee channels should be free from interference from Wi-Fi transmissions, that is, channels 25 and 26 (the two rightmost ones). However, there is no assurance that using channels 25 and 26 solves the interference problem. For example, two channels might not be enough to allow the coexistence among several geographically overlapping PANs. In addition, though in North America ZigBee channels 25 and 26 can be really assumed free from Wi-Fi transmissions, in other regions such as Europe and Asia all Wi-Fi channels can be used, thus covering the complete set of ZigBee channels.

A further aspect making the coexistence of Wi-Fi and ZigBee difficult is the different allowed transmission power. In fact, the maximum Wi-Fi output power can be up to 100 times higher than the maximum allowed ZigBee transmission power (100 mW versus 1 mW). The same consideration holds for Wi-Fi and Bluetooth devices belonging to Classes 2 and 3.

6. Proof of Concept

To put the ideas expressed in the previous sections into practice, we have realized a small testbed involving all the elements of the architecture. The SHG, being the core and most innovative element, has been built from scratch. Two DSANs have been implemented using two sets of ZigBee and Bluetooth devices. Finally, to illustrate the potentials of expansion and customization of our architecture, we have defined and implemented the "home automation" package, a specific SIP event package for the domotics framework.

6.1. SIP-Based Home Gateway. The only requirements for building the SHG are the sufficient processing power and memory to run the software and the capability to interface with the technologies of the particular sensor networks to control.

With regard to the former aspect, we used a generic single-board computer (SBC) with a Texas Instrument AM 3730 processor (ARM Cortex-A8) running at 720 MHz with 256 MB of DRAM and 256 MB of NAND flash memory. As it will be shown in Section 7.2, this hardware is more than adequate. To give the SHG the physical interfaces towards the wireless networks, a ZigBee module has been embedded into the board and connected to the main processor via a serial interface; then a Hama Bluetooth adapter and a Wi-Fi card were inserted into the two USB ports. Figure 6 shows the prototype SHG.

The SHG software was built on top of Linux (with kernel 2.6.36), which provides the necessary support and development tools (e.g., a SIP library, the interface drivers). The software that implements the SHG functionalities has been written from scratch using the C++ language and then cross-compiled for the ARM platform. A multithreaded approach has been followed. Each user request is handled in parallel by a different thread. This helps improving the scalability performance of the SHG.

The internal software architecture of the SHG is reported in Figure 7. Starting from the top, the first object we meet is the SIP interface. This is nothing more than the SIP software (the GNU oSIP and eXosip libraries), which extracts the user's commands from the SIP messages and passes them to the next module in the form of plain text strings. These are then translated into the proper DFA actions by the translation module, which fetches the set of available DFA actions from the DFA Library. The output of this module is fed to the SHG engine, where we have placed the intelligence for executing the user's directives in the proper way. This is typically achieved via the creation of a series of elementary DSAN commands to be delivered to the various DSAN elements. The set of available elements and commands is retrieved from the device database. The SHG engine then passes the DSAN commands to the various DSAN managers, which are in charge of translating them into the technology-specific commands and performing all the operations to ensure that the specified actions are fulfilled. Finally, the ZigBee, Bluetooth, and Wi-Fi interfaces are the software modules (a custom software for ZigBee, the BlueZ stack for Bluetooth, and the Linux drivers and tools for Wi-Fi) that

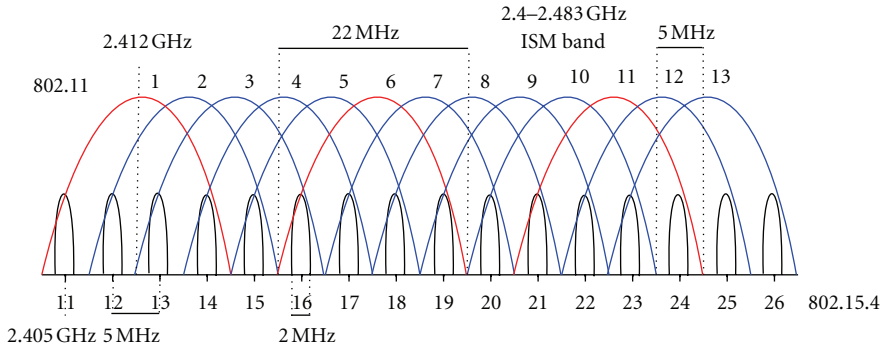


Figure 5: Channel occupancy of 802.11 and 802.15.4 systems.

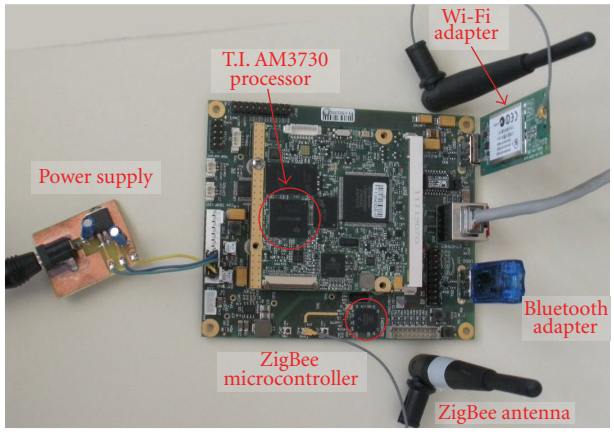


Figure 6: A photo of the SHG prototype, with the indication of the main components.

pilot the physical objects that are connected to the various sensors and actuators.

The device database (DdB) holds the set of available DSAN objects, with the related properties (e.g., commands, location, technology). The DdB is filled and kept up to date by the DSAN managers, which are aware of the number and types of devices connected through the various DSAN interfaces. Further information, such as the physical location of each device, can be inserted at configuration time either by the user or by the service provider.

The operations in the reverse direction, that is, from the DSAN networks to the SIP interface, are analogous to the ones mentioned above. The notifications from the sensors are passed, by means of the DSAN managers, to the SHG engine, which decides what actions are to be taken. For example, a new command might be issued towards the DSAN, or an information message can be sent to the user (or both). In the latter case, the message is passed to the translation module and finally to the SIP interface.

6.2. The Wireless Networks. This section briefly describes the setup of the two DSANs and of the Wi-Fi local area network. A few essential technical details are also given.

6.2.1. The ZigBee DSAN. The nodes of the ZigBee sensor network are based on the Freescale MC1322x board, which integrates a 32-bit ARM-7 MCU and a low-power 2.4 GHz transceiver. The fully compliant ZigBee stack provided by Freescale was installed on the nodes.

A custom application that supports environmental data collection (temperature and pressure), remote light control, and message routing has been developed on top of the ZigBee stack by means of the ZigBee Cluster Library (ZCL) functions. The APS ACK feature (an end-to-end acknowledgment mechanism) was enabled to make the ZigBee transmissions reliable.

Ambient data is retrieved both on regular time basis and on demand, and both approaches are available to the user, who can either subscribe to this event or ask the SHG to check a specific sensor value. As for remote light control, the MC1322x boards are equipped with an array of LEDs, which was used to mimic a multilevel light. For both ambient data collection and light control, we defined a set of textual commands. Combining them with the name of a room allows the user to set the desired light level or retrieve the sensor reading.

An important aspect of the ZigBee system is that it provides for a mechanism, known as *binding*, to connect endpoints (an "endpoint" is a logical wire connecting distributed applications residing on different nodes). Binding creates logical links between endpoints and maintains this information in a binding table. The binding table also has information about the services offered by the devices on the network. The ZigBee coordinator (ZC) typically holds the binding table for the whole network. A notable advantage of this structure is that it allows the implementation of the *service discovery* procedure via bindings. The services available inside the ZigBee network can thus be discovered directly within the ZigBee domain, without resorting to any additional software or external entities. With specific reference to the SIP control plane, this means that there is no need to port the SIP registration procedure to the ZigBee network, since this would be a duplication of the ZigBee service discovery.

6.2.2. The Bluetooth DSAN. The Hama Bluetooth adapter connected to the SHG board embeds a version 2.0 compliant

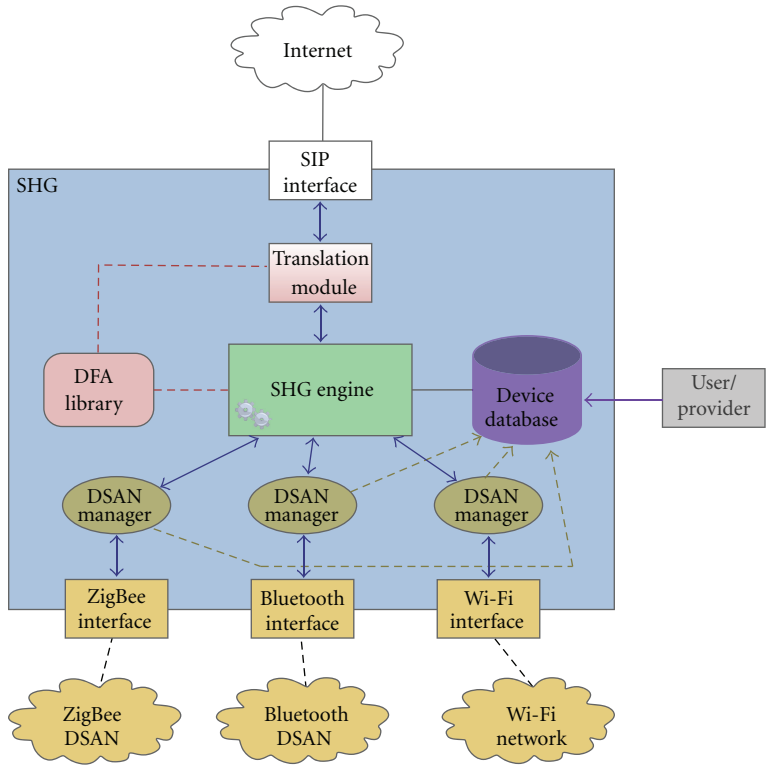


Figure 7: The software modules building the prototype SHG.

chipset supporting the EDR feature. It is a Class 2 device, with 2.5 mW (4 dBm) of output power allowing for an approximate range of 10 meters and a physical bit rate of 3 Mbps. To operate this device, we took advantage of the Bluetooth Linux stack (BlueZ), which gives support for basic operations such as scanning and pairing. On top of these basic functionalities, we built the Bluetooth interface, which is capable of listing and managing the connected devices.

For the purposes of validating the domotics system, we set up an audio streaming test. A Bluetooth-enabled headset (Sony DR-BT101) was used as the client device. The audio streaming was handled directly by the BlueZ (on the SHG side) and the headset, by means of the A2DP profile.

On the SIP-based control plane, we defined and implemented some simple commands, such as listing of the available content and playing an audio stream on the Bluetooth headset.

6.2.3. The Wi-Fi Local Area Network. To build the Wi-Fi LAN, we used two adapters based on the Ralink RT3572 chipset, a IEEE 802.11a/b/g/n compliant card. One of the adapters was installed on the SHG and the other on a common laptop PC. The drivers from the latest "compat-wireless" package have been used to pilot the card.

We set up a private IBSS network on one of the 2.4 GHz channels. The use of an IBSS topology rather than an "infrastructure" one is justified by the shorter set-up times (mostly in terms of driver and software configuration) but has no impact neither on the traffic at the transport and application layers nor on the physical layer mechanisms. The SHG and the PC are therefore two "peer" stations.

Traffic on the Wi-Fi connection has been generated by means of common test applications, such as FTP or iperf.

6.3. A Domotics Event Framework. The SIP Event Notification Framework (ENF) standardized in RFC 3265 [21], and later augmented by RFC 3903 [22], provides just the procedures that enable notification of events (as outlined in Section 3.1) but do not define any specific "event package." Indeed, a few packages for the SIP ENF have currently been ratified. Among them, the Presence package [25] is probably the most popular and also the one that is implemented in some widely available SIP clients. However, this package does not suit well the needs of a domotics environment, as it provides just a single elementary functionality (the presence of a given user) and refers to the bare ENF, without taking advantage of the `PUBLISH` method.

To test our domotics system with a complete and flexible Publish/Subscribe-Notify paradigm, we built a new package, named "home automation." The basic features of home automation are similar to the ones of Presence, but our package employs the PUBLISH method too. We designed it to embed a customized XML text, like the one illustrated in Figure 8, which contains domotics specific data (such as the values read by some ambient sensors). In this particular example, the XML snippet is sent from the SHG to an *enhanced client* to report about the readings of the sensors in the *Lab* room and also the current light level. Note that

```
<device room = "Lab"
        name = "dimmablelight">
    <attrib name = "Level"
            value = "33">
    </attrib>
</device>
<device room = "Lab"
        name = "ambientsensor">
    <attrib name = "Temperature"
            value = "20">
    </attrib>
    <attrib name = "Pressure"
            value = "308">
    </attrib>
</device>
```

Figure 8: Figure 8: Sample XML for the home automation event package.

the tags implement a possible functional naming abstraction of the DFA layer. Clearly, this XML scheme can be replaced with any other kind of text format, like REST or SOAP (the ones employed by the ZigBee Gateway [26]).

In order to correctly handle this package, we also built a customized ESC server. We employed Kamailio, an open-source SIP server released under GPL, to which we made some modifications. The changes mainly consisted in adding the specific home automation keywords to let it recognize the home automation package in a similar fashion to any other package.

Note that the XML text is not touched by the ESC (only a formal check is done) but is passed directly to the subscribers by means of the `NOTIFY` messages. Hence, SIP is immediately able to deliver this information using the existing infrastructure.

6.4. SIP Clients. We developed a test SIP client that supports the full Publish/Subscribe-Notify paradigm and the Home Automation package described in Section 6.3. One such client is in all aspects a SIP-compliant software, but with the extra feature that can control the DSAN with its native semantic.

6.5. SIP Servers. Servers build the necessary infrastructure for SIP to work properly. In our proof of concept, we employed two different servers. An external registrar and a proxy server provided by *iptel.org* were used as a sample of a preexisting SIP network element. This server is compliant to existing SIP standards and is completely unaware of the nature of our domotics testbed.

A customized SIP server was built in our lab by means of the Kamailio open-source software. As explained in Section 6.3, this was necessary to provide support for our home automation event package. Hence, this server is representative of a domotics-aware element in the SIP infrastructure. We called this server the enhanced notification server (ENS).

7. Performed Tests

The performed tests can be divided in two sets. The first series was aimed at assessing the performance of the prototype SHG in terms of capacity, scalability, and processing delay. The objective of the second set instead was to verify the amount of interference among the wireless interfaces on board of the SHG and the impact on the SHG performance.

Before discussing the tests, we outline the deployed networks and the environment where the tests have been carried out.

7.1. Network Topology. All tests have been carried out within the premises of the Dipartimento di Ingegneria dell'Informazione of the University of Pisa, Italy. This might indeed constitute a good environment for both kinds of tests: applications such as smart energy, building automation, and intrusion detection systems fit well this kind of structures, and we might indeed expect to find in the department several devices using different radio technologies working at the same time.

The realized testbed is made of five ZigBee sensor nodes, including the ZigBee coordinator (ZC), which is embedded in the SHG board as already shown in Figure 6. The physical location of the nodes is illustrated in Figure 9. All ZigBee nodes have a wireless path to the ZC. Due to the indoor environment, the nodes *Stairs*, *Office*, and *Corridor* use a multihop path. The Bluetooth headphones (*bths*) are placed in the same room of the SHG, approximately 8 meters apart; the PC acting as a Wi-Fi station (*sta1*) is placed in a room adjacent to the one with the SHG. We checked that the Bluetooth and Wi-Fi devices, as well as the *Lab* node, are within the operation range of the SHG. *sta0* represents the Wi-Fi adapter connected to the USB port of the SHG.

7.2. Performance of the SHG. We assessed the performance of the SHG in terms of two metrics: the number of served user requests per second (in short: SURPS) and the average response time.

To compute the first metric, we connected the SHG to a varying number of clients through our 100 Mbps local area network. Every client was programmed to send a continuous flow of 100 requests using the `MESSAGE` method. Each request is cast as soon as the previous response is received from the SHG (we recall that a response is implemented with a distinct `MESSAGE` transaction). In this way the SHG always has a pending request to process for each client. The auxiliary SIP procedures, such as registration, have been excluded in order to measure the raw SHG capacity. For the same reason, we did not connect the SHG to any real DSAN but implemented a fake interface that returns a response as soon as it receives a command. In practice, with reference to Figure 7, the processing path stops at the ZigBee interface. The Bluetooth and Wi-Fi networks were left inactive.

The collected numbers of total SURPS and mean SURPS per client, averaged over ten experiments, are reported in Figure 10 as a function of the number of connected clients. Focusing on the red lines (labeled "eXosip"), we can see that

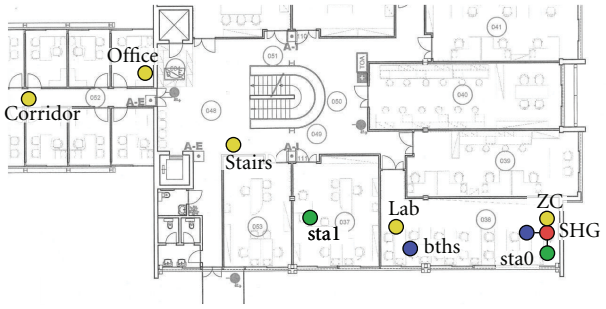


Figure 9: Map of the Dipartimento di Ingegneria dell'Informazione with the position of the ZigBee, Bluetooth, and Wi-Fi nodes (yellow, blue, and green discs, resp.); the SHG is also shown (red disc).

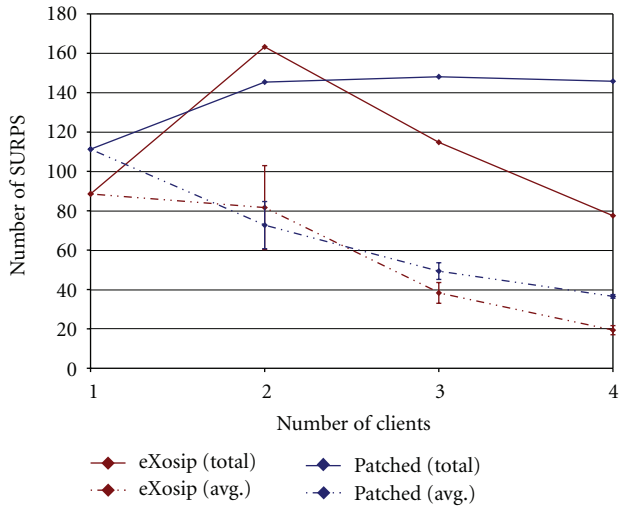


Figure 10: Total and average number of user requests per second served by the SHG; the standard deviation among the clients is also reported.

when a single client is connected, this can enjoy a service rate that is around 89 requests per second. This number can undoubtedly be deemed adequate not only for any human-based activity but also for any sensible automated application (see, e.g., [11]). In case of two clients, the number of total SURPS is almost doubled, but when further clients are added, there is a sudden performance drop. When four clients are connected, the total SURPS are even less than the single client case.

We have explored the reasons for such a tremendous degradation and found that it was due to the eXosip library integrated into the SHG. Without delving into the software details, this library presents some structures and timeouts that slow down the entire system when eXosip is called to serve many requests at the same time. We thus devised a simple patch that bypasses these shortcomings and repeated the SURPS test.

The results for the amended version are also shown in Figure 10 (the blue lines, labeled "patched"). The performance of the SHG has improved for almost any number of connected clients (it has slightly worsened for the two-client case only). More remarkable, however, is the fact that the trend in the number of SURPS is now much smoother and, above all, that the total number of SURPS reaches a stable level—it floors to about 146 SURPS. This means that the performance of the SHG is not appreciably influenced by the number of clients. Hence, we can reasonably affirm that the SHG can scale to serve many requests from different clients at the same time.

With the second performance test, we analyzed the behavior of the SHG from an internal point of view. We measured the time that elapses between the reception of a request `MESSAGE` and the issue of the response `MESSAGE`. The measurement was carried out with a single client, with the auxiliary SIP procedures at work, but still with the Bluetooth and Wi-Fi networks kept idle. We used two configurations. The first one is still based on the fake interface, whereas the second setting is an operative scenario with a real ZigBee DSAN attached. To keep the things simple, however, the ZigBee DSAN is composed of two nodes only: the coordinator (physically soldered to the SHG board) and a device node in direct communication range. The ZigBee network operated on channel 25, which is the most free from external interference sources.

The first row of Table 1 shows the processing times of the SHG in the two configurations. The difference is apparent, with them being apart by almost two orders of magnitude. This result does not leave much room for speculation and clearly identifies the bottleneck of the system with the domotics sensor network.

In the second row of Table 1, we have reported the performance of the SHG software when run on a generic PC based on an Intel Core i3 processor running at 2.66 GHz with 4 GB of RAM. The purpose of these figures is to provide a comparison with a "high-end" hardware. The PC is somewhat slower in running the software but is faster when the actual ZigBee network is attached. The "software" gap can be ascribed to the scarce optimization of both the code and the hardware, whereas the "DSAN" gap comes from the different connection with the ZigBee coordinator: serial (slower) on the SHG prototype and USB (faster) on the PC.

7.3. Effect of Interference. To check the effect of the interference on the domotics system, we set up a sort of "use-case" scenario. We assumed that the Wi-Fi and Bluetooth networks are used to deliver different but massive data to the user(s). Specifically, a FTP or HTTP transfer is conveyed over the Wi-Fi connection, whereas an audio streaming is performed by means of the Bluetooth devices. The SHG thus acts as the source of the data, and its Wi-Fi and Bluetooth interfaces work mainly as transmitters. Such a scenario can be mapped, for example, to a file download from the Internet (the FTP transfer) and a user listening to a song retrieved from a local repository (the audio streaming). As for the ZigBee DSAN, this is used to send commands to the sensors spread across the house. We exploit the *request/response* paradigm implemented via the double SIP `MESSAGE` transactions (as illustrated in Section 3.1.1). Hence, the SHG and the sensors alternate the roles of source and destination of the traffic.

Table 1: Processing delay of the SHG.

Hardware	Fake interface	Real ZigBee DSAN
SHG prototype	11.0 ms	177 ms
i3-based PC	34.8 ms	103 ms

Since the weak link in the chain is the ZigBee connection, our effort was mostly targeted at measuring the effect of the two "stronger" technologies, that is, Wi-Fi and Bluetooth, on the performance of the ZigBee subsystem and consequently on the capability of the user to control and have feedback from the ZigBee DSAN.

The test was organized in a similar manner as the performance experiment described in the previous section. A SIP client sends a continuous flow of 100 requests to the SHG via the local 100 Mbps Ethernet LAN. Each request is sent as soon as the previous response is received. No requests nor responses are lost in this segment of the system. The auxiliary SIP procedures (registration, publish, etc.) have been disabled, as they do not have any influence on the radio interference. The SHG then translates and casts the requests over the ZigBee network. Only one ZigBee sensor node is used for the test. This is sufficient for the purposes of the test, as the interference mostly occurs in the first wireless hop.

As for the wireless segment, we placed the Wi-Fi network on channels 1 or 11 and the ZigBee DSAN either on channel 25 or on channel 15. We did not test the system under overlapped ZigBee and Wi-Fi channels because we believe it is logical to assume that a deployed system will be smart enough to avoid such clearly troublesome kind of allocation. Also, we did not test the full range of possible combinations, which is not the purpose of the present work—the reader interested in this kind of analysis can refer to [14].

We collected four performance parameters: the average command service time registered on the client (in short: service delay), the average and the peak command execution time on the ZigBee interface (in short: execution delay and peak delay), and the number of lost commands (i.e., either lost requests or lost responses; we made ourselves certain that the losses can only occur on the ZigBee network).

To monitor the activity on the 2.4 GHz spectrum, including possible external interference sources (e.g., other Wi-Fi networks), we used the AirView2-EXT ISM-band spectrum analyzer (http://www.ubnt.com/airview). A screenshot of the power level in the test area has been taken before performing every experiment, to check whether strong external interferences are present and thus avoiding biased results.

Table 2 reports the outcome of the tests. The first test, labeled "0", is a preliminary test, used to benchmark the system when solely the ZigBee network is active (on channel 25). We can see that no commands are lost and that the peak execution delay is just a few milliseconds greater than the average. This indicates that the behavior of the ZigBee network is quite stable. Also, the average service and the execution delays differ only by 3 ms.

In the next test (1), we activated both the Bluetooth and the Wi-Fi networks, with Wi-Fi placed on channel 1, that is, the farthest possible from the ZigBee one. In this case, the interference is mostly due to Bluetooth, which covers the whole 2.4 GHz band. The performance drop is apparent, with an increase of 12% in the average time. The peak delay is the value that changed most, as it is now almost seven times the average execution delay. Thus, the ZigBee network can still bring all commands to completion, but its response time has become quite unpredictable. In absolute terms, however, even the highest values (1.268 s) can be deemed acceptable.

Table 2: Interference performance of the SHG.

Metric	Test 0	Test 1	Test 2	Test 3
Service delay	179.4 ms	202.0 ms	835.9 ms	937.5 ms
Execution delay	176.5 ms	197.2 ms	824.4 ms	913.6 ms
Peak delay	181.4 ms	1268 ms	5538 ms	5291 ms
Lost commands	0	0	0	0

In test (2) we moved the Wi-Fi emissions closer to the ZigBee ones; that is, we put Wi-Fi on channel 11. In theory, there is still no overlapping between the ZigBee and the Wi-Fi channels. But in fact the ZigBee segment is heavily penalized, as proved by the values in Table 2. The average delays reach almost 1 second, with the peak execution delay going beyond 5 seconds. For some applications these values might be critical, for the user annoying. Note, however, that no commands are lost.

The reason for these figures lies in the long timeouts and the numerous retries that are allowed at the ZigBee application and MAC layers. For example, the default application retry timeout is 1.5 seconds, and the allowed number of retries is 3, both at the MAC and at the application layer. Thus, the ZigBee network, which is highly hampered by Wi-Fi, can take advantage of several attempts to deliver each packet, and consequently the overall transmission time grows very large.

To have a confirmation that Wi-Fi interferes with ZigBee even in nonoverlapping channels, we repeated the test by moving Wi-Fi to channel 1 and ZigBee to channel 15. The numbers of this test (3), which are very similar and even worse than the previous ones, indeed corroborate this fact.

8. Conclusions

The paper presented an architecture and a home gateway for realizing a domotics system with heterogeneous devices and user terminals. The architecture is based on the use of SIP as the common control plane and is centered on the SIP-based home gateway. A functional addressing scheme and an abstract translation layer (called DFA) are used to make the underlying technology transparent to the user. The DFA is the glue between the DSAN domain and the SIP world and simultaneously allows to separate the implementation of the SIP and DSAN interfaces. In addition, by choosing to expose a single SIP URI to the user (the SHG one), the system increases the user-friendliness and can be easily extended to large deployments. Note that this single-URI approach is neither an intrinsic feature of SIP nor of the domotics

concept itself. Rather, it is a notable advantage of the way we built our architecture and the SHG. The positive impact of this approach is greater as the network grows larger.

We have built a proof of concept that includes the prototype SHG, three standard ZigBee, Bluetooth, and Wi-Fi networks, a newly defined SIP event package, and a customized event state compositor.

The performance of the SHG has been assessed in terms of served user requests per second, processing delay, and average and peak service delay. The effect of having the three wireless interfaces on the same board that operate on the same frequency band has also been evaluated.

The results proved the SHG ability to support a considerable number of requests per second, also from a different number of clients. Thus, the developed prototype can indeed be employed for large deployments, as it does have the ability to scale to any realistic requirement.

On the interference side, it emerged that ZigBee suffers the presence of both Bluetooth and Wi-Fi. Yet, while the former technology produces just a relatively small performance degradation, the presence of Wi-Fi is definitely more cumbersome, as the ability of the ZigBee network to accomplish its task in short times is heavily hampered. Though the weakness of ZigBee is well known, it is remarkable that this occurs even when Wi-Fi and ZigBee operate on channels that are nominally separated from each other. Our experiments showed a tremendous performance degradation when ZigBee and Wi-Fi are on adjacent channels. Nevertheless, by means of a proper configuration, we have also proved that it is possible to avoid command losses.

Acknowledgments

This work was supported by the Italian Ministry of Instruction, University and Research (MIUR) under the PRIN 2009 Research Project GATECOM. The authors would like to thank Luca Boggioni and Alessio Del Chiaro for their help in developing the prototypes and running the tests.

References

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo et al., "SIP: session initiation protocol," RFC 3261, Internet Engineering Task Force, 2002.

[2] K. Sohraby, D. Minoli, and T. Znati, *Wireless Sensor Networks: Technology,Protocols, and Applications*, John Wiley and Sons, 2007.

[3] R. Musaloiu-Elefteri and A. Terzis, "Minimising the effect of WiFi interference in 802.15.4 wireless sensor networks," *International Journal of Sensor Networks*, vol. 3, no. 1, pp. 43–54, 2008.

[4] A. Sikora and V. F. Groza, "Coexistence of IEEE802.15.4 with other systems in the 2.4 GHz-ISM-band," in *Proceedings of the IEEE Instrumentation and Measurement Technology Conference*, vol. 3, pp. 1786–1791, May 2005.

[5] T. Luckenbach, P. Gober, S. Arbanowski, A. Kotsopoulos, and K. Kim, "TinyREST: a protocol for integrating sensor networks into the internet," in *Proceedings of the Workshop on Real-World Wireless Sensor Networks (REALWSN '05)*, June 2005.

[6] S. Krishnamurthy, "TinySIP: providing seamless access to sensor-based services," in *Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MobiQuitous*, July 2006.

[7] S. Krishnamurthy and L. Lange, "Enabling distributed messaging with wireless sensor nodes using TinySIP," in *Ubiquitous Intelligence and Computing*, J. Indulska, J. Ma, L. Yang, T. Ungerer, and J. Cao, Eds., vol. 4611 of *Lecture Notes in Computer Science*, pp. 610–621, 2007.

[8] M. Alia, A. Bottaro, F. Camara, and B. Hardouin, "On the design of a SIP-based binding middleware for next generation home network services," in *Proceedings of the OTM 2008 Confederated International Conferences, CoopIS, DOA, GADA, IS, and ODBASE*, pp. 497–514, 2008.

[9] R. Acker, S. Brandt, N. Buchmann, T. Fugmann, and M. Massoth, "Ubiquitous home control based on SIP and presence service," in *Proceedings of the 12th International Conference on Information Integration and Web-Based Applications and Services (iiWAS '10)*, pp. 759–762, November 2010.

[10] B. Bertran, C. Consel, P. Kadionik, and B. Lamer, "A SIP-based home automation platform: an experimental study," in *Proceedings of the 13th International Conference on Intelligence in Next Generation Networks (ICIN '09)*, Bordeaux, France, October 2009.

[11] B. Bertran, C. Consel, W. Jouve, H. Guan, and P. Kadionik, "SIP as a universal communication bus: a methodology and an experimental study," in *Proceedings of the IEEE International Conference on Communications (ICC '10)*, May 2010.

[12] S. Y. Shin, H. S. Park, S. Choi, and W. H. Kwon, "Packet error rate analysis of zigbee under WLAN and bluetooth interferences," *IEEE Transactions on Wireless Communications*, vol. 6, no. 8, pp. 2825–2830, 2007.

[13] I. Howitt, V. Mitter, and J. Gutierrez, "Empirical study for IEEE 802.11 and bluetooth interoperability," in *Proceedings of the IEEE Vehicular Technology Conference (VTS SPRING '01)*, pp. 1109–1113, May 2001.

[14] R. Garroppo, L. Gazzarrini, S. Giordano, and L. Tavanti, "Experimental assessment of the coexistence of wi-fi, zigbee, and bluetooth devices," in *Proceedings of the 12th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WOWMOM '11)*, pp. 1–9, Lucca, Italy, june 2011.

[15] H. Schulzrinne, X. Wu, S. Sidiroglou, and S. Berger, "Ubiquitous computing in home networks," *IEEE Communications Magazine*, vol. 41, no. 11, pp. 128–135, 2003.

[16] D. Bonino, E. Castellina, and F. Corno, "Automatic domotic device interoperation," *IEEE Transactions on Consumer Electronics*, vol. 55, no. 2, pp. 499–506, 2009.

[17] F. Genova, M. Gaspardone, A. Cuda, M. Beoni, G. Fici, and M. Sorrentino, "Thermal and energy management system based on low cost wireless sensor network technology, to monitor, control and optimize energy consumption in telecom switch plants and data centres," in *Proceedings of the 4th International Conference on Telecommunication-Energy Special Conference (TELESCON '09)*, May 2009.

[18] A. Brown, M. Kolberg, D. Bushmitch, G. Lomako, and M. Tthew, "A SIP-based OSGi device communication service for mobile personal area networks," in *Proceedings of the 3rd IEEE Consumer Communications and Networking Conference, CCNC 2006*, pp. 502–508, January 2006.

[19] D. J. Cook, J. C. Augusto, and V. R. Jakkula, "Ambient intelligence: technologies, applications, and opportunities,"

Pervasive and Mobile Computing, vol. 5, no. 4, pp. 277–298, 2009.

[20] B. Campbell, J. Rosenberg, H. Schulzrinne, C. Huitema, and D. Gurle, "Session initiation protocol (SIP) extension for instant messaging," RFC 3428, Internet Engineering Task Force, 2002.

[21] A. B. Roach, "Session initiation protocol (SIP)-specific event notification," RFC 3265, Internet Engineering Task Force, 2002.

[22] A. Niemi, "Session initiation protocol (SIP) extension for event state publication," RFC 3903, Internet Engineering Task Force, 2004.

[23] "IEEE Standard 802.11-2007," December 2007.

[24] "IEEE Standard 802.15.4-2006," September 2006.

[25] J. Rosenberg, "A presence event package for the session initiation protocol (SIP)," RFC 3856, 2004.

[26] The Zigbee Alliance, "ZigBee Gateway Standard," 2010, http://zigbee.org/Standards/ZigBeeNetworkDevices/Overview.aspx.

Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2012, Article ID 863521, 10 pages
doi:10.1155/2012/863521

Research Article

Delay-Tolerant, Low-Power Protocols for Large Security-Critical Wireless Sensor Networks

Claudio S. Malavenda,[1,2] F. Menichelli,[2] and M. Olivieri[2]

[1] *Large Systems BU, SELEX Sistemi Integrati, 00131 Rome, Italy*
[2] *Department of Information Engineering, Electronics and Telecommunications, Sapienza University of Rome, via Eudossiana 18, 00184 Rome, Italy*

Correspondence should be addressed to M. Olivieri, olivieri@diet.uniroma1.it

Received 1 August 2012; Accepted 23 October 2012

Academic Editor: Bruno Neri

This paper reports the analysis, implementation, and experimental testing of a delay-tolerant and energy-aware protocol for a wireless sensor node, oriented to security applications. The solution proposed takes advantages from different domains considering as a guideline the low power consumption and facing the problems of seamless and lossy connectivity offered by the wireless medium along with very limited resources offered by a wireless network node. The paper is organized as follows: first we give an overview on delay-tolerant wireless sensor networking (DTN); then we perform a simulation-based comparative analysis of state-of-the-art DTN approaches and illustrate the improvement offered by the proposed protocol; finally we present experimental data gathered from the implementation of the proposed protocol on a proprietary hardware node.

1. Introduction

In recent years, wireless sensor networks (WSN) research has grown exponentially spreading through several fields of science, from circuit design to algorithm design, antenna design, and protocol design. The main constraints that a generic WSN node has to deal with can be summarized by its limited computing resources and its energy consumption requirements. While the computing resources and corresponding consumed energy tend to grow with silicon technology improvements, available energy budget does not advance very fast with battery technology or can even be bounded in other cases (i.e., energy scavenged from the environment). Power management must therefore be taken into account at every level of the design of any WSN.

In security-critical applications, the deployment of large networks faces—among others—the implications of delay variability on the correct operation of security algorithms. This paper illustrates the results of an industrial work on the analysis, optimization, implementation, and experimental testing of a dedicated protocol featuring delay tolerance and energy efficiency for large WSNs in the security application domain.

This paper is organized as follows: in Section 2 we present an overview on wireless sensor networking with particular regard to delay-tolerant networking (DTN) and specifically to the DTN logical link control (LLC) layer, with the aim of stating general and direct hints for the protocol design. Section 3 illustrates a dedicated DTN simulation framework and presents simulation results on existing widely used protocols compared with the newly proposed protocol. Section 4 presents the test methodology and the experimental results on a working application of the new protocol implemented on a hardware sensor node architecture used in security market.

2. Overview on DTN Design

2.1. WSN Protocol Stack General Issues. A WSN is a dynamic, self-configuring network composed of interconnected, battery-powered embedded systems. The main characteristics of these kinds of systems are scalability, self-organization, self-configuration, adaptation, exception-free operation, and communication failure tolerance [1]. All these requirements have to be implemented in an embedded device (node)

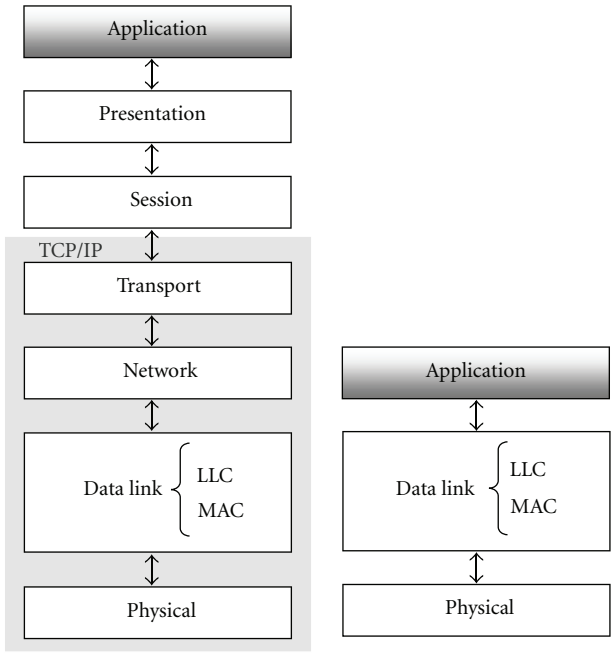


Figure 1: Comparison of a common OSI model and a reduced one for WSN application.

that typically has limited energy budget, computing power, storage capacity, transmission range, and bandwidth.

As formerly investigated in several works for embedded systems communications [2, 3], an important aspect for achieving the above goal is to reduce the protocol stack of a common OSI model in order to have a faster computation and smaller number and size of packets to transmit. Figure 1 shows the difference between a typical OSI model (left side) and an adapted one (right side) for WSN systems.

A shorter stack is a simplification from the point of view of network design and computation load within the node, but complicates the software development of services offered to applications. In fact, a shorter stack implies that applications directly drive layers close to the physical one and requires much more complex workarounds to achieve "high layer-like" functionalities. Such complexity is usually hidden to the application developer in common OSI-based network stacks (e.g., TPC/IP networks) where lower layers are seen as black boxes. As a consequence of such limiting factor in application development, the huge production of WSN protocols in the last years has often adopted the classical approach ignoring the optimization of the stack at lower layers (shorter stack) and often producing a heavy weighted protocol stack that does not fit with the most common operating constraints for WSN [4]. On the contrary, the proposed approach fully adopts a shorter stack approach.

In addition to the generic framework of computation-optimized shorter stack, the following main characteristics of WSN protocols that differ from a common TCP/IP network have been addressed in the new protocol.

(i) *Intermittent connectivity:* a connection path among nodes does not always exist, and available links are time varying. So the network could be partitioned in several and different parts during its life.

(ii) *Relatively long and variable delay:* propagation delay among network nodes is relevant. Delay is not fixed and can vary according to network traffic and link quality. This condition tends to cause failure in protocols that are based on quick data/ack return.

(iii) *Lossy link:* the end-to-end communication suffers a high error rate due to several physical causes. Packets are frequently lost in hop-to-hop connection.

2.2. Asynchronous Networking. Taking in mind the above starting point, a *synchronous* MAC [5], either slotted or frame based, could be hardly suitable because of the synchronization needed among nodes. This result comes from years of experimentation and protocol testing during the development of the proposed protocol. In fact, synchronous MAC needs the successful communication among nodes of periodic packets that synchronize neighbors for subsequent transmissions. Each sensor node would start this communication with a delay according to a fixed cycle started with the shared time-synchronization event.

Conversely, *asynchronous* MACs [5] do not impose restrictions on when a sleep/active cycle is taking place. Neighbors therefore do not need to coordinate their cycles and consequently wake up independently of each other. This avoids the overheads and bookkeeping associated with running a time synchronization protocol and a global scheduler, as in a synchronous MAC, at the expense of requiring the sending nodes to arrange a rendezvous with the intended receiver whenever it wakes up. As a consequent drawback, asynchronous protocols suffer of congestion problems when the density of active nodes becomes high due to the intrinsic nature of its relaying mechanism. In fact, the number of neighbors becomes a pointer to discover potential congestion in the network. However, asynchronous MAC remains the preferred way in our application context where the reliability of the medium and of communication timing cannot be continuously known (DTN application context).

2.3. Delay-Tolerant Networking. DTN responds to the need to deliver messages in networks characterized by probable lack of end-to-end connection paths, either proactively available [6] or reactively established with conventional routing protocols. Thus, these networks must operate without the assumption that there is a permanent connection or instantaneous end-to-end paths between the source and the destination node.

This is quite common in those WSNs where disconnections among nodes occur dynamically. The main causes of node disconnections can be attributed to *mobility of nodes* and *sparse network*. In the first case, the assumption is that a WSN node has mobile capabilities, and its movement can lead to lack of connectivity when the node moves out of the radio range of any of its neighbours. The sparse network case may occur even when a WSN comprises only static nodes due to node malfunction, battery discharge, change in node's functional state, or node switch to sleep mode following

a duty cycle different from its neighbours. The resulting distribution of nodes creates holes in network topology. In our target application context, both mobility of modes and sparse network condition must be assumed.

The solutions to this issue are usually some elaboration of the basic *store* and *forward* scheme. In this direction, the concept of *Data Mule* [7], as a specialized vision for the general DTN case, is sometimes introduced in mobile networks. A Data Mule is a mobile WSN node with high data storage capability, high throughput, and ability to move in order to establish connection among unconnected islands or networks.

As shown in Figure 2, the Data Mule collects messages incoming from a network island, when it is in proximity to that island. If an incoming message is addressed to a node of the network that is within the Data Mule's transmission range, the Data Mule will forward the message. Otherwise, the Data Mule stores the message and physically moves towards the destination node's network island to start forwarding the stored messages.

As for the routing layer, typical routing protocols for WSNs are divided in reactive and proactive ones [6]. Proactive routing sets up predefined paths from all source nodes towards all possible destination nodes before starting to route data messages. Reactive routing establishes a connected end-to-end path on demand, when a generated message needs to be routed from its source towards a destination node. In a typical DTN network application, a path typically cannot be preestablished, so that reactive routing is the mandatory choice.

2.4. Overhead Sources in Delay-Tolerant Networking. For the power efficiency of a WSN protocol, a critical aspect is the minimization of bytes/packets transmitted in the network for its correct operation, in order to minimize the energy spent in transmission. As a result, a primary design criterion is the overhead of communications exchanged for protocol specific purposes and of other energy consuming operations. In the specific context of DTNs, the main sources of overhead that must be addressed and minimized are as follows.

(i) Idle Listening Overhead. The time spent listening to the medium and receiving nothing. While communications are usually a quite rare event, the receiving radio must be kept on every time a packet could be incoming; otherwise it would miss some of the messages being sent to it. This is the main source of energy waste as typical radios consume much more energy in receive mode (even when no data is arriving) than in sleep mode. In asynchronous protocols, the idle listening can be computed with the receiving time-window that occurs each WOR period over the effective receiving periods that catch radio packets.

(ii) Overhearing Overhead. The nature of the wireless medium implies broadcast communication among neighbor nodes, so that all neighbors of the destination node will receive the same packet. Overhearing these messages is a waste of energy: the node spends energy to receive a packet that is not addressed to it. This source of overhead becomes problematic in dense networks. These kinds of deployments are common, for instance, when sensing range is smaller than communication range so that a high number of nodes are inside the communication range, in order to cover the smaller sensing range.

(iii) Collision-Related Overhead. When a packet collision occurs, usually it implies the retransmission of the collided packet and a waste of energy. In this respect, *traffic fluctuations* in WSN where packets are generated just in case of an event to report can cause a peak of transmission load, network congestion, and frequent retransmissions. Also back-off period calculated with random generators can still produce contentions, because collisions can still occur between the carrier sense time and the effective transmission. The protocol overhead usually uses the RTS/CTS handshake to implement collision avoidance, but it is considered prohibitive in comparison to the small, 32-byte WSN payloads leaving the hidden-terminal problem unaddressed.

(iv) Protocol Overhead. All headers/footers and control packets are overhead, that is, a waste of energy in front of zero data information transmitted. The minimization of these fields/packets type is the scope of a good WSN design.

The optimization of these parameters has driven the design of the proposed protocol, tested in Section 4.1.

2.5. Performance Metrics. Performance metrics are not easy to define in WSN due to its unique properties. Common metrics used in wireless communication, like *fairness* and *throughput*, might not be meaningful because WSN nodes can cooperate and because raw data transmission is a rare application in WSN.

We used the following metrics to measure protocol performances in both simulator and implementation, whose results are reported in Section 3.2.

(i) Latency. Time delay between the message transmission from the source node and the first arrival of the message to the destination node.

(ii) Delivery Ratio. Ratio of the number of successfully delivered data packets over the number of packets generated by source-nodes.

(iii) Overhead. Number of redundant packet copies that are disseminated in the network and the extra control packets exchanged for protocol specific purposes.

We note, for completeness, that also another metric can be defined.

(iv) Network Efficiency. The sum of all packet copies generated by all of the relaying nodes (including the source node) in order to deliver one packet (other definitions can be application dependent).

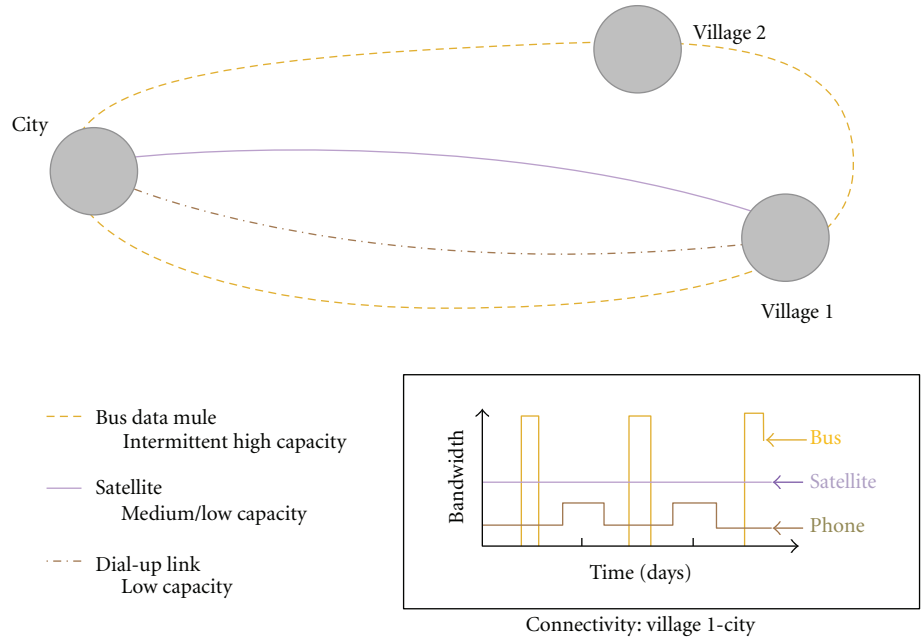


Figure 2: Comparison of common bandwidth versus time data exchange in intermittent island and medium/low capacity but connected island [8].

However, the definition of *network efficiency* is quite variable and it is usually related to a specific application. That is why it will not be used as a comparison in Section 3.2.

3. Simulation-Based Analysis of Existing DTN Protocols

3.1. Protocols under Analysis. The most widely used DTN protocols reported in the literature [7, 9–12] are listed below:

(i) Direct Diffusion,
(ii) First Contact,
(iii) Epidemic,
(iv) Fuzzy Spray,
(v) PRoPHET,
(vi) MaxProp,
(vii) Spray and Wait (and variants),
(viii) Scar,
(ix) FAD,
(x) Rapid.

The above protocols can be classified according to the map in Figure 3. The gray cell represents typical characteristic of a DTN protocol. The lower part of the map inherits the characteristics at the highest level. In the following, a brief description of each characteristic is listed in the map.

Single Transmission. A packet is transmitted in broadcast and just once after its creation.

Multitransmission. A packet can be transmitted more than once from the same node.

Replication. A packet can be relayed from a receiving node. This is the first step for multihop communication.

Queue Management. From this level, the management of relays starts. In this case, the relay of the packet is accomplished according to a queue that can be managed on the sender node in several ways. For instance, a simple management can be a FIFO queue, but parameters on node energy are taken into account.

Delivery Probability. According to the specific protocol, every packet is associated with a probability that can, for instance, be linked to the destination of the packet, or according to the routed path. If the probability associated to the incoming packet is greater than a certain percentage, the packet is relayed or not.

Limited Copies in Network. This characteristic limits the number of copies that can simultaneously coexist in the network. Protocols that implement this characteristic vary on the rules adopted to limit copies in the network.

We performed a comparative analysis of the above protocols on a commercially available simulator [10], in order to have a basis on which we can build the mechanisms that could lead to an optimization of the network in the target application context.

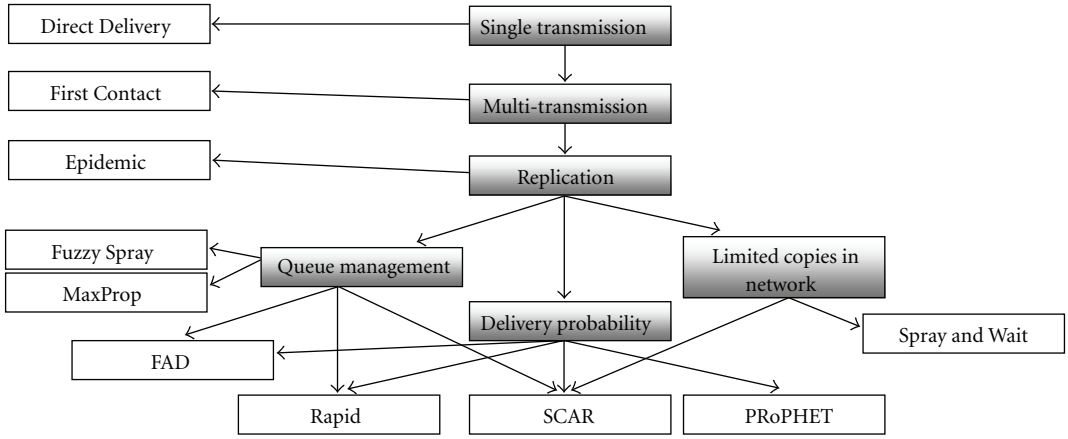


Figure 3: Map of most widely used DTN protocols.

3.2. Simulation Results. The diagrams in Figures 5 and 6 present the results of the comparison based on the previously chosen metrics.

Figure 4 shows latency measures for all tested protocols. In a subsequent analysis, we limit the exploration to a set of the most performing ones, specifically MaxProp, Prophet, and Spray and Wait. PRoPHET is representative of protocols implementing only the data forwarding scheme, Spray and Wait only the controlled replication scheme, and MaxProp both.

It is possible to remark that due to the limited buffer size, PRoPHET significantly suffers from message discarding, while Spray and Wait, by limiting the total number of copies, can in any case achieve good performance.

From Figure 4, we can also note that the selected protocols mark two extremes of a range of latency values, while other protocols are positioned between them according to the scheme implemented. Other protocols having performance outside this range are considered out of interest.

Figures 5 and 6 present the performances of the selected protocols, regarding delivery ratio and overhead, respectively.

Considering the trade-off between performance and power consumption, the Spray and Wait protocol comes out to be the one with the lowest overhead while maintaining average results on delivery ratio and delay, in the target application domain. As a consequence of the analysis, the newly developed protocol has been an optimization of Spray and Wait.

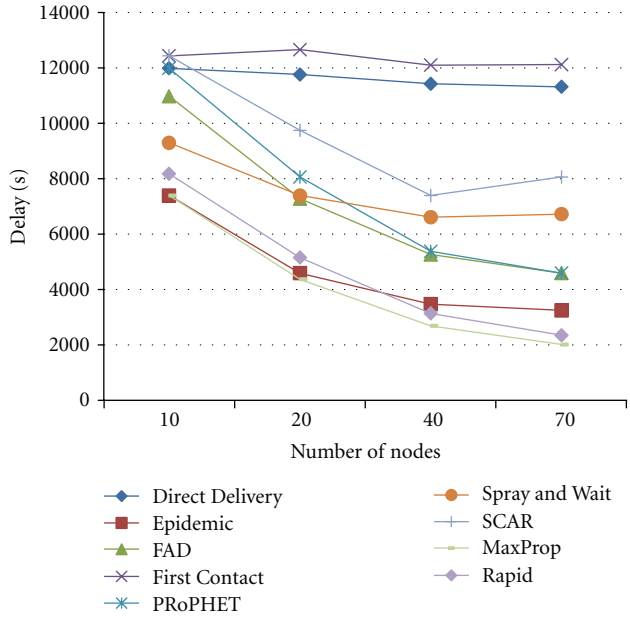


Figure 4: Latency result comparison.

4. New Protocol Simulation and Experimental Testing

4.1. Analysis on a Dedicated State-Accurate Simulator for DTN Protocols. In order to have a deeper control on the developed protocol, with state-level accuracy, and in order to have a better energy model, a custom simulator framework for DTN protocols has been developed. OMNET++ 4.2 [13] has been chosen as a starting framework. The simulator has been layered over the basic OMNET API, without any other add-on installed.

The simulator aims at modeling, with state-level accuracy, the hardware of a WSN node with particular regards to the radio and microcontroller states, in order to produce accurate results on their power consumption. It has been designed in order to provide a dynamic positioning of WSN nodes over a simulated area.

Connections among nodes are dynamically established according to physical parameter relative to each single node, which is modeled with a particular antenna gain and receive sensitivity. Working frequency is used to model the communication range achievable from each node according to the mutual position of the nodes.

Figure 7 shows a test topology used to verify the reliability of the simulator. The graphical rendering of OMNET++

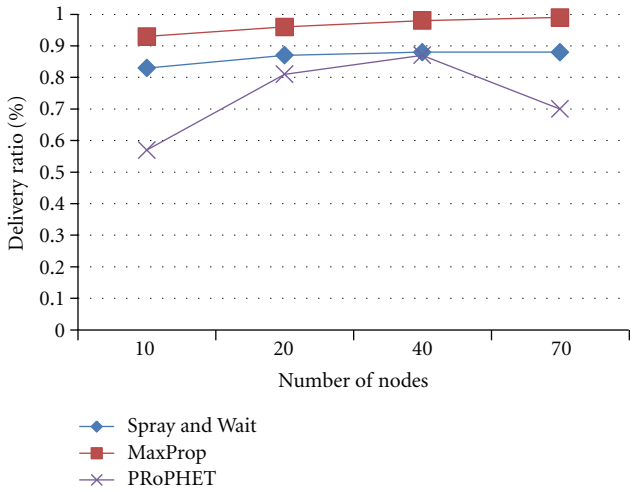


Figure 5: Delivery ratio result comparison.

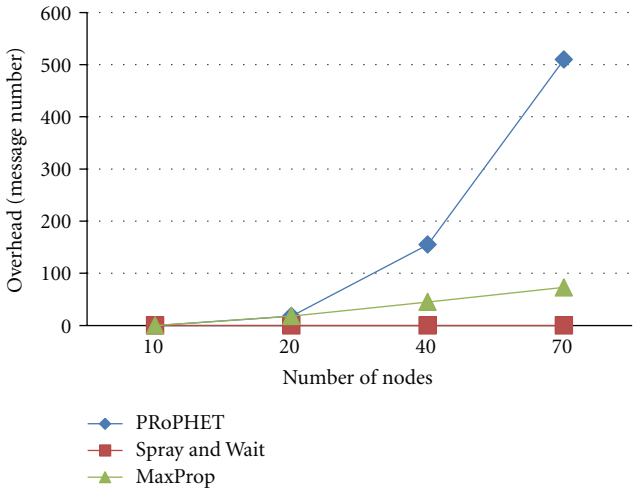


Figure 6: Communication overhead result comparison.

shows the topology of fixed nodes disposed on a virtual field. Each position of the virtual field is mapped with a coordinate reference in a 3D virtual space. In this way it is possible to map the mutual distance between nodes.

A configuration file describes the physical characteristics of each node joining the WSN with the possibility of inheriting standard ones, in the case that no particular physical parameters have been specified for a node.

The first use of the simulator has been done to verify timing on packet delivery and model packet exchanging among nodes with a first version of the selected protocol, in order to validate the simulator with known results and acquire more data on the simulated network.

As it is possible to see in Figure 9 that it never occurs that a node starts transmitting while another one in its visibility range is yet in transmission phase. Moreover, it is possible to see the packet relay period of 1 second when no collisions occurs which correctly model the protocol used.

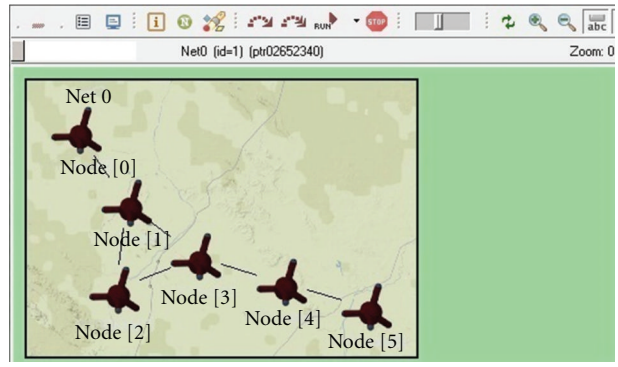


Figure 7: Network topology—A screenshot with fixed nodes.

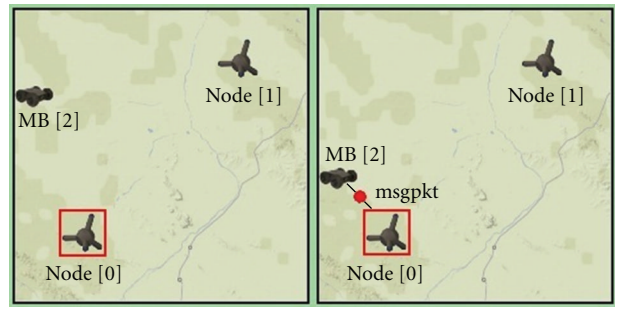


Figure 8: Network topology—mobile UGV and fixed nodes.

Since the protocol is a DTN one and well fits for communication among mobile nodes, a mobile node modeling feature has been developed and introduced in the framework as well (Figure 8).

4.2. Hardware Test Session No. 1. The testing of the protocol implemented in a real commercial hardware WSN node has been divided into different set of testing sessions.

The first session deals with node power consumption, by analyzing the duty cycle and power consumed during different transmission phases. All testbeds have been set up in the WSN laboratory of SELEX Sistemi Integrati (formerly ElsagDatamat) in an air-conditioned environment at 25°C.

4.2.1. Testbed Setup. The testbed is settled up with a single MasterZone [8] node.

The node has been programmed in order to configure its transceiver in Wake-on-Radio status: the radio goes in reception mode for a short period (15 ms) and after that stays in sleep state for 800 ms.

Sporadically, the node performs a transmission. In this configuration, it is possible to monitor the consumption of the node during its reception and transmission phase.

The measurement of the current consumed by the node is performed with a current probe in order to produce a temporal log of measures and distinguish the power consumed between each phase.

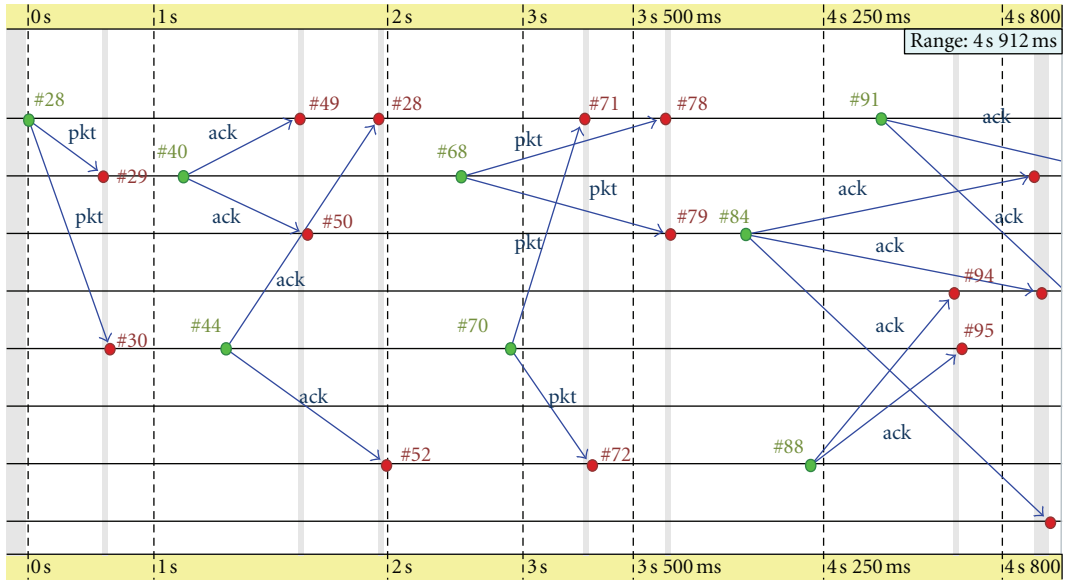


Figure 9: Network timing monitoring view.

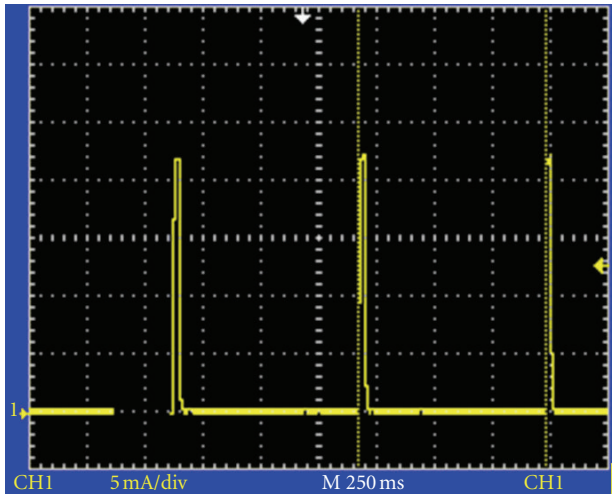


Figure 10: Receiver WOR period—power consumption test result.

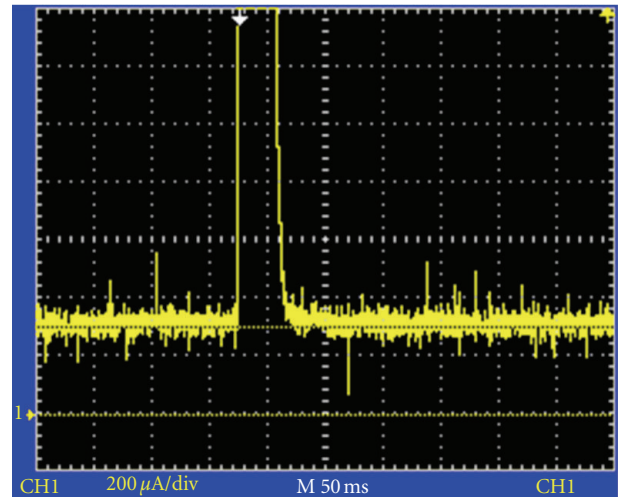


Figure 11: Sleep power consumption test result.

The log obtained has been splitted and reported in Figures 10 and 11 in order to focus on each particular Rx and Tx phases.

4.2.2. Results and Analysis. The first measure concerns the WOR timing. As from Figure 10, every 800 ms the power consumed by the node shows a high step due to the state change from "idle/sleep" to "receive."

Figure 11 shows a detail of the power consumption trace where we can observe a background consumption of 200 uA in sleep mode and a raising peak of 22 mA in active receive mode.

Figure 12 illustrates the corresponding test for a transmission phase. We can see a first phase of 30 ms with a power consumption of 30 mA for the CSMA/CA phase at the beginning of the transmission phase, and a 900 ms transmission phase with a 23 mA of power consumption at −15 dB of Tx power.

It is possible to observe that the transmission phase has a bounce in energy consumption. It is due to the fast change of states in the transmitter radio (from idle to transmitter). Results obtained in this test comply with the expected results.

4.3. Hardware Test Session No. 2. The second set of tests has been set up using a single node. This test deals with the correct functioning of the radio of the node.

4.3.1. Testbed Setup. The target measures in this test aim at the detection of the sensitivity of the node radio receiver

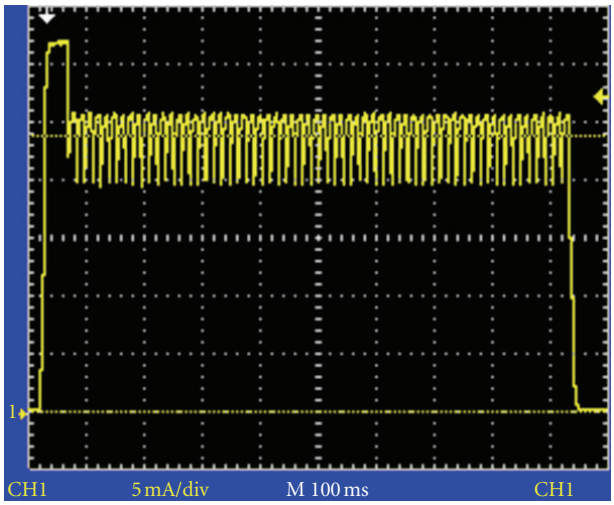


Figure 12: Transmitter power consumption test result.

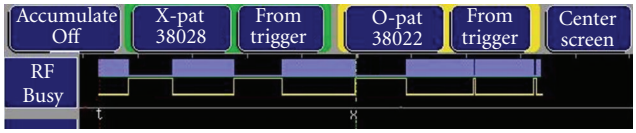


Figure 13: Sensitivity measurement.

and confirm the correct functioning of the CSMA strategy adopted.

The measures are accomplished by means of a logic state analyzer linked to a control IO of the node under test. This pin is directly controlled by the microcontroller and reports the status of the radio channel in use (i.e., if the radio channel is busy or free, according to a predefined threshold on received power). The threshold has been set to the minimum value available: in this way the pin will take a low-logic state when the minimal energy is detected in the received channel.

The antenna plug of the node has been connected directly through a coaxial cable (50 Ohm, SMA connector) to a RF generator which provides a radio signal directly injected in the reception circuits of the node. The direct connection from the RF generator avoids errors in the measurement that could be introduced by a free air link.

4.3.2. Results and Analysis. The results collected prove a −90 dBm sensitivity of the node. In fact, going below this threshold causes the pin that monitors the status of the air to bounce independently from the actual injection of RF.

In Figure 13, it is possible to see the correct response obtained from the node when −90 dBm of RF power is injected.

The first line monitors the transmission of RF from the generator. The absence of glitch in the white signal means a good clear channel measurement. Going below this power, the white line starts to bounce: the node cannot really discern a free channel from a busy one. This test attests the sensitivity of the node at −90 dBm.

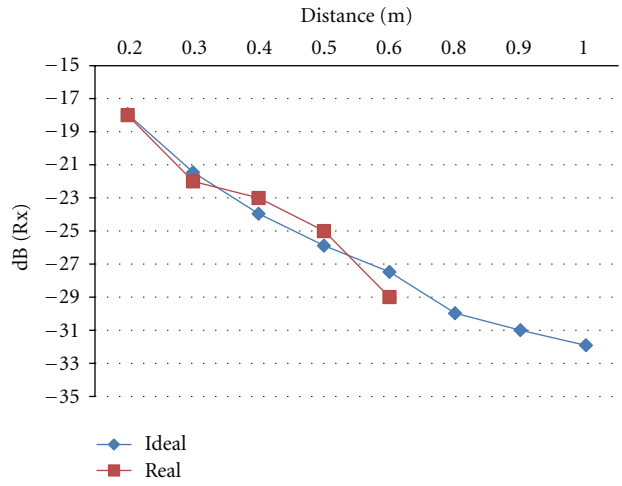


Figure 14: Measurements achieved versus expected ones.

4.4. Hardware Test Session No. 3. The third set of tests has been set up on a two node network: the target is the measure of the distance achievable by a point-to-point transmission.

4.4.1. Testbed Setup. This testbed is set up with two MasterZone nodes [8] suitably programmed.

The first one has been configured to periodically transmit a packet. In this test environment, the content of the packet is not important, but just the fact that it is received or not by the second node, since we are going to measure physical values related to RF transmission.

The second node is configured to remain in reception state, read the RSSI level of received packets, and translate it in dBm values. This translation has been tuned in advance using reference values from datasheets. The node sends the data to a PC via an RS232 serial connection, where they are timestamped and logged.

4.4.2. Results and Analysis. Figure 14 shows a plot of actual measurements towards ideal values. The ideal values (in blue) depict the expected dBm power at the receiver according to a Free Path Loss law with a Tx power of 5 dBm and an antenna gain of −6 dBm at a working frequency of 420 MHz.

As we can see from the figure, the mapping of ideal values and the real ones is quite 1 : 1 with a few dBm difference.

Assuming that the measurements follow this trend, the threshold level of −90 dBm may be reached at 800 m distance between the transmitter and the receiver. More tests should be conducted with greater distances between nodes to confirm the trend with distances next to the maximum one achievable.

4.5. Test Session No. 4. The fourth session has been set up on a multihop testbed and the target parameter has been the measure of the delay. In this testbed, we have a source node, a relaying node, and a sink node. All nodes are visible to each other. The test aimed at verifying a simple relay functioning.

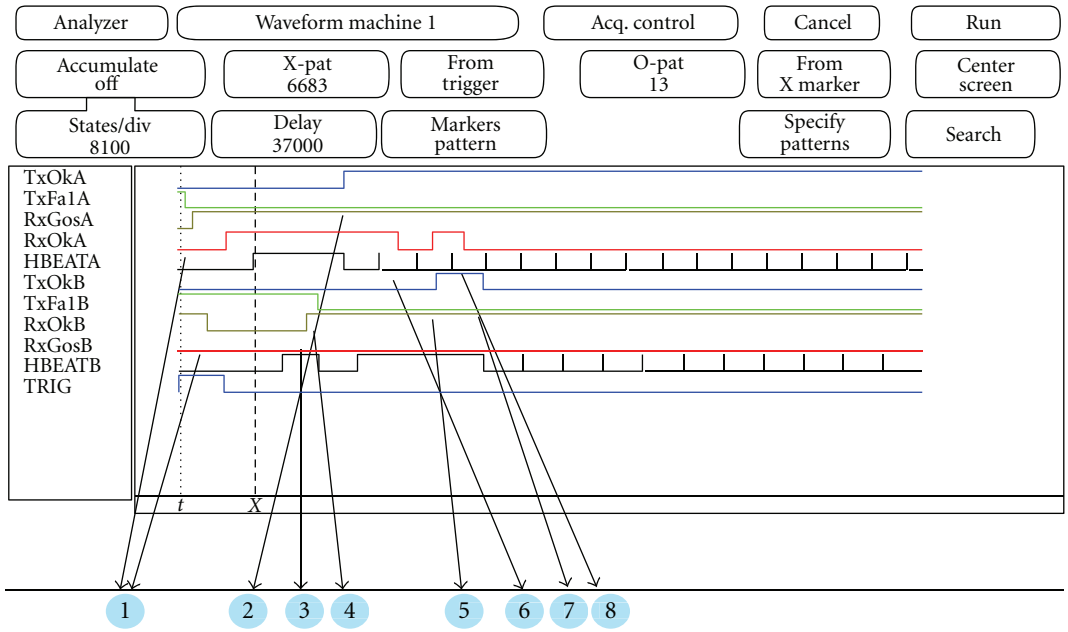


Figure 15: Multihop signal test.

4.5.1. Testbed Setup. This test bed is set up with two MasterZone nodes [8] suitably programmed (node A and B) and one node interfaced with a PC (TRIG).

All nodes have been configured to test the multihop functionality of the protocol when incoming messages are relayed to neighbor nodes.

The TRIG node transmits "ping" packets under control of the PC. This node will not take part in any other radio handshaking. The "ping" packet received by node A is relayed to node B.

The state analyzer will log all control pin on both nodes in order to catch a clear picture of the handshaking. The test aims at examining if the routing with a minimal set of nodes reflects the expected behavior.

4.5.2. Results and Analysis. Figure 15 reports the result of the test conducted with the configuration just described. The cyan balloons highlight the following communication facts.

(1) Nodes A and B receive ping command from the sink node (A receive twice in the same slot).

(2) A answers to the sink node with a delay of 2.42 sec.

(3) B receives the answer transmitted by A (the signal toggle monitor the end of a transmission).

(4) B tries to forward the ping request issued by the sink node but senses the air occupied.

(5) B forwards the sink request.

(6) A receives the forwarded request from the sink node and filters it because already received.

(7) B transmits the answer from A.

(8) A receives its own answer from B and just drops it.

This handshake reflects the expected behavior.

A logic state analyzer has been connected to the nodes to monitor handshaking occurring between node A and B. Five I/O pins have been configured on each node to monitor events on nodes according to Table 1. The events monitored deal with a successful or failed transmission started from the node, a successful reception, or a reception of a packet yet stored in the reception queue (ghost packet). The signal Hbeat reveals the internal timing of the node.

Table 1: Signal meaning mapping.

Signal name	Meaning
TxOk	Toggle after a successful transmission
TxFal	Toggle after a failed transmission
RxOk	Toggle after the reception of a packet
RxGos	Toggle after the reception of a filtered packet
Hbeat	Low when the node is in sleep mode

5. Conclusions

In this paper, we first presented a comparison between different delay-tolerant protocols for WSN systems. Starting from the definition of the metrics of interest for WSN performance analysis found in the literature, we compared different delay-tolerant protocols.

A wide range of protocols have been investigated through available simulators. After a set of simulation results and comparisons according to the chosen metrics, the most promising one has been selected to develop a new custom protocol.

In order to reach a more accurate control of the simulation and incorporate a wider set of simulation parameters, the simulation platform has been switched to a more versatile one. The code of the custom protocol based on the selected one has been implemented in the new simulation environment. The first simulation results have been collected with fixed and mobile nodes. These tests have confirmed the suitability of the protocol for an actual implementation.

Finally the custom protocol has been ported on a proprietary platform: the correct implementation has been validated through a set of tests on timing, handshaking and power consumption of the developed node, confirming the expected results and paving the way to further subsequent development.

Acknowledgments

This work was supported by SELEX Sistemi Integrati, a Finmeccanica Company. Special thanks are due to to Luca di Donato for his support.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] B. Maaref, S. Nasri, and P. Sicard, "Communication system for industrial automation," in *Proceedings of the IEEE International Symposium on Industrial Electronics (ISIE'97)*, vol. 3, pp. 1286–1291, July 1997.

[3] W. Hou, S. Hu, R. Li, and M. Fei, "A wireless industrial networks protocol stack with time synchronization and node positioning," in *Proceedings of the IET Conference on Wireless, Mobile and Sensor Networks 2007 (CCWMSN'07)*, pp. 1077–1080, Shanghai, China, December 2007.

[4] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," in *Proceedings of the ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'04)*, vol. 34, no. 4, pp. 145–158, New York, NY, USA, September 2004.

[5] C. K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*, Prentice Hall, New York, NY, USA, 2001.

[6] "Proactive and reactive routing in wireless sensor networking," http://it.wikipedia.org/wiki/MANET.

[7] M. Demmer, E. Brewer, K. Fall, S. Jain, M. Ho, and R. Patra, "Implementing delay tolerant networking," Intel Corporation, 2004, http://www.dtnrg.org/docs/papers/demmer-irb-tr-04-020.pdf.

[8] http://www.selex-si-uk.com/pdf/Masterzone.pdf.

[9] K. A. Harras, K. C. Almeroth, and E. M. Belding-Royer, "Delay tolerant mobile networks (DTMNs): controlled flooding in sparse mobile networks," in *Proceedings of the 4th IFIP-TC6 International Conference on Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communication Systems (NETWORKING'05)*, pp. 1180–1192, May 2005.

[10] "ONE," simulator web page, http://www.netlab.tkk.fi/tutkimus/dtn/theone/.

[11] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the ACM SIGCOMM Workshop on Delay-Tolerant Networking (WDTN'05)*, pp. 252–259, August 2005.

[12] B. Pásztor, M. Musolesi, and C. Mascolo, "Opportunistic mobile sensor data collection with SCAR," in *Proceedings of the IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS'07)*, pp. 1–12, Pisa, Italy, October 2007.

[13] OMNET++, http://www.omnetpp.org/.

Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2012, Article ID 184783, 14 pages
doi:10.1155/2012/184783

Research Article

Selective Forwarding Attacks against Data and ACK Flows in Network Coding and Countermeasures

Yuanyuan Zhang[1,2] and Marine Minier[1]

[1] *CITI laboratory, INSA-Lyon, INRIA, Université de Lyon, 69621 Lyon, France*
[2] *Department of Computer Science and Technology, East China Normal University, No. 500 Dongchuan Road, Shanghai 200241, China*

Correspondence should be addressed to Yuanyuan Zhang, yyjess@gmail.com

Received 27 April 2012; Revised 30 July 2012; Accepted 27 September 2012

Academic Editor: Gildas Avoine

Network coding has attracted the attention of many researchers in security and cryptography. In this paper, a well-known attack *selective forwarding attack* will be studied in network coding systems. While most of the works have been dedicated to the countermeasures against pollution attacks where an attacker modifies intermediate packets, only few works concern selective forwarding attacks on data or acknowledgment (ACK) packets; those last ones are required in network coding. However, selective forwarding attacks stay a real threat in resource constraint networks such as wireless sensor networks, especially when selective forwarding attacks target the acknowledgment (ACK) messages, referred to as *flooding attack*. In the latter model, an adversary can easily create congestion in the network and exhaust all the resources available. The degradation of the QoS (delay, energy) goes beyond the capabilities of cryptographic solutions. In this paper, we first simulate and analyze the effects of selective forwarding attacks on both data flows and ACK flows. We then investigate the security capabilities of multipath acknowledgment in more details than in our original proposal (Zhang et al., 2011).

1. Introduction

Network coding is a very active field of both information theory and networking for information dissemination. It consists in encoding a message into several packets and transmitting those packets in an oriented multicast way through the network to the destination. The intermediate nodes can also combine the received packets. It has been shown that network coding could reach the maximum possible information flow in a network. Network coding is also very interesting for security. Many works have been interested in demonstrating the security capacity of network coding. Two security worlds coexist, and the border is delimited by the adversary capabilities. Network coding can be used to bring secrecy if the adversary eavesdropping capabilities are bounded (see [1–3]). Otherwise, cryptography and security must be used to defeat more powerful adversaries [4–6]. This paper falls in the second class of works related to network coding and security.

In network coding, two information flows are identified: the data flow and the acknowledgment (ACK) flow. Both flows can be targeted by an adversary with different consequences. An adversary attacking the data flow wants to affect the messages produced by different sources and decoded by the destinations. An example of such an attack is *pollution attacks* [6]. Many works have proposed countermeasures against *pollution attacks* [4, 5, 7–10]. Another classical attack on data flow is selective forwarding attack where an adversary drops/delays all or part of the data packets he receives. As shown in [11], this kind of attacks is defeated by network coding due to its intrinsic multipath nature. In this paper, we first show by simulations this result; selective forwarding attacks on the data flow are inefficient when network coding is employed in the network.

Finally, attacks against the ACK flow have less attracted the attention of the security community. It does not mean that threats against the ACK flow are less dangerous than those on the data flow, quite the contrary. Threats against the

ACK flow can be partially defeated by some cryptographic techniques. But it is not enough to prevent attacks against the quality of services (QoS). Attacking the ACK flow can create congestion or exhaust the nodes energy by flooding the network with useless packets. Up to our knowledge, Dong et al. [6, 11] are the only ones referring to attacks against the ACK flow in network coding with the DROP-ACK attack [6]. The threats considered in this paper have all the same consequence: flooding. Unfortunately, the solutions found against flooding in classical networks [12] are all dedicated to TCP and cannot be applied in our context.

In this paper, we first give simulation results concerning the effects on selective forwarding attacks first targeting the data flow and second the ACK flow. From those simulations, we observe that first and as expected selective forwarding attacks targeting the data flow are inefficient when network coding is activated in the network and second that attacks against the ACK flow could be really efficient. We then propose a dedicated mechanism based on multipath routing of ACK packets to discard flooding attacks when the adversary drops or delays the ACK packets. We then provide some results concerning global evaluation of the security of network coding when selective forwarding attacks on data and on ACK flows are combined.

In Section 2, network coding and selective forwarding attacks are described as well as related works. Section 3 presents our network and adversary models and describes our multipath ACK back strategy to prevent flooding attacks together with some implementation issues. Section 4 gathers all our simulation results concerning selective forwarding attacks and flooding attacks against first classical network coding (without our multipath strategy) and second network coding with our multipath strategy. We finally show that classical network coding is efficient against selective forwarding attacks and that our network coding multipath ACK strategy is efficient against flooding attacks and sum up those results in Section 5.

2. Preliminaries

In this section, we remind the basic elements on network coding and the related work on flooding attacks.

2.1. Network Coding. The seminal work on network coding was done by Ahlswede et al. in [13]. The main aim of network coding is to find optimal information dissemination in a network. It has been shown that network coding can also improve the network resilience against communication failure, for example, erasure, [14, chapter 1]. Wireline and wireless networks can benefit from network coding. For more details on network coding and on the problems solved by this technique, the readers can consult [14–16].

An important topic in network coding is linear codes: packets exchanged by the nodes are linear combinations of the data to be transmitted over a given finite field. Random linear network coding [17] has particularly attracted attention. The coding process is as follows. Let us assume a network viewed as a graph with a source node and some destination nodes. Let us denote $D = (d_1, d_2, \ldots, d_n)$ a data of kn bits viewed as a vector of n fragments $d_i \in \mathbb{F}_{2^k}, i \in [1, n]$. The messages $m_j = h_j \| p_j$ transmitted by the source and the relaying nodes in a scheme using random linear network coding consist in a header h_j and a payload p_j:

$$p_j = \sum_{i=1}^{n} \alpha_{i,j} d_i, \tag{1}$$

where the coefficients $\alpha_{i,j}$ are chosen randomly over $\mathbb{F}_q$ with $q = 2^u$ the favorite choice in the literature. The header h_j contains all the coefficients $\alpha_{i,j}$ which describe the payload:

$$h_j = \left(\alpha_{1,j}, \ldots, \alpha_{n,j}\right). \tag{2}$$

The source and the relaying nodes apply the coding process infinitely until they receive an acknowledgment (ACK) from all destinations. All destinations run the decoding process: a Gaussian elimination or any other methods for solving linear systems of equations (not described here). In network coding, we have an implicit "*data flow*" which transmits data from the sources to the destination and a *feedback/acknowledgment flow* which carries the ACK from the destination to the sources.

Finally, network coding problems are divided into two classes: *intra-flow* and *inter-flow*. Intraflow network coding corresponds to the example described above: a single message and one or several sources. Interflow network coding combines different messages from different sources at the level of intermediate nodes. This problem is also known as source network coding.

Classically, network coding is used with an oriented multicast strategy that could be compared with a partial flooding of information. This partial flooding allows to obtain the maximum possible information flow in the network.

Generally, in most network environments, the mechanism of transmission of the ACK packets usually employs the routing protocol at the lower routing layer by default. This simplified treatment is enough for most of the upper layer transmission demands in most networks such as TCP/IP because the retransmission will compensate the loss of ACK. However, in network coding environments, the source node continues sending encoding packets until it receives an ACK to confirm the correct decoding at the sink node, so it is crucial to guarantee its arrival.

2.2. Classical Attacks against Network Coding. Three attacks are dedicated to network coding in the security literature: *packet pollution attack* [6, 11], *drop-data packets attack* [11] (also known as selective forwarding attack), and DROP-ACK *attack* [6]. In a pollution attack, an adversary injects invalid packets into the data flow. The adversary exploits the capacity of network coding to spread information at his own advantage. The invalid packets are carried through the network to be only discarded by the destination in the best case. The resources, for example, bandwidth, energy used to carry these packets are lost. Such an attack is extremely powerful in resource-constrained networks such as wireless

sensor networks (WSNs). Many papers are devoted to find countermeasures to pollution attacks [4, 5, 7–10].

Selective forwarding attack is a well-known and very harmful attack in wireless multihop networks for example described in [18]. In a selective forwarding attack, a compromised node refuses to forward some of the packets in its outstanding buffer, such as control information or data packets in order to cut off the packets propagation. An extreme example of this attack is a two-step attack where first a malicious node attracts most of the local traffic using, for example, false neighbors information, and then the malicious node completely suppresses the received packets transmission provoking what is usually known as a *black hole attack*. Selective forwarding attacks will not always happen on the data flow but also on controlling packets such as HELLO packets or acknowledgment packets. When it is applied on ACK, we talk here about *flooding attacks*.

Selective forwarding attacks have been studied [11] in the context of network coding where the adversary drops or delays packets of the data flow. By its intrinsic nature, network coding process uses several routes to transmit a message, and the consequences of this attack will be essentially to introduce a delay as shown in [11] but not to prevent the data to reach the destination. Some additional methods [19] coming from the routing world can also help improving the damaged throughput and to decrease the delay.

A DROP-ACK attack [6, 11], or flooding attacks as it is referred throughout the paper, targets the ACK flow. Everything happens after a destination successfully decodes D and starts to forward an ACK. Attacking the ACK flow can be particularly interesting for the adversary: preventing the ACK to reach the source can increase the congestion in the network, prevent a given source to transmit new information, or exhaust the energy of all nodes forwarding the packets (see Figure 1).

From the perspective of the classical man-in-the-middle adversary model, three attack strategies are possible against the ACK flow: injecting/modifying ACK, dropping/removing ACK, and delaying ACK. The last two attacks are the ones leading to a flooding attack.

(a) Injecting/Modifying ACK. Charlie attempts to forge an ACK packet and sends it to Alice. She can believe that Bob has received enough information to recover D. Such attacks can be prevented by a proper use of cryptography, that is, by using a message authentication code (MAC) [20–22] and key distribution [23].

(b) Dropping/Removing ACK. Charlie is seen as a black hole attacker by destroying any ACK packet. Charlie can also just modify the ACK delivery path to prevent the packet to reach Alice. As a result, Alice continues indefinitely sending encoded packets to Bob and so wastes resources. This attack is very difficult to detect.

(c) Delaying ACK. In this case, instead of dropping the ACK packet, Charlie has just to delay the delivery of the packet. This behavior is difficult to distinguish from the selfishness behavior when nodes want to reduce their own energy consumption. As a result, this attack increases the time needed to pass to the next set of packets, and it implies a node energy waste and additional transmission delay.

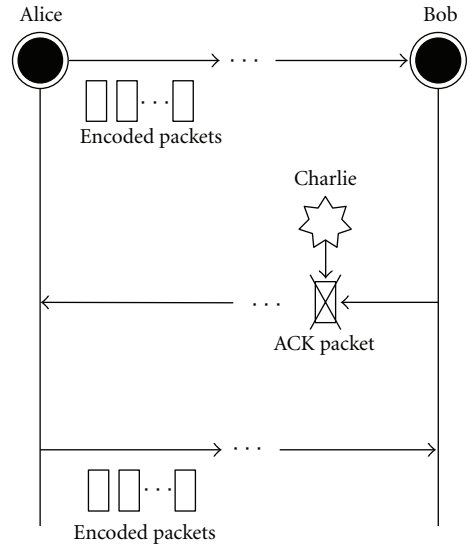


Figure 1: An example of flooding attack. Alice is the source who attempts to send encoded packets to the destination, Bob. Bob is supposed to forward an ACK to Alice once he successfully decodes a message. The adversary, Charlie, drops or delays the ACK: Alice never stops to transmit packets to Bob.

3. General Assumptions, Implementation Aspects, and Our Proposal

In this section, we provide all the hypotheses made concerning the network, the adversary models, and the implementation of the network coding process. We also provide in Section 3.3 our multipath ACK back strategy to discard flooding attacks.

3.1. General Network Assumptions and Adversary Models. In our proposal, we focus on large-scale static wireless sensor networks as case study with two types of nodes: low-power sensor nodes and a single collecting point which we call the sink.

In our approach, all low-power sensor nodes are exactly the same. In our implementation, we use a general multistream unicast scenario as a network coding mechanism. Every sensor node has 100 raw messages to be encoded and delivered to a single destination which is the sink. So, from this point, we talk about the destination or the sink without distinction. A source sensor node continuously sends one encoded packet per second until it receives the ACK from the sink, and then it starts sending the encoded packets of the next raw message. Meanwhile, all the sensor nodes also play the role of forwarding nodes in the network. The encoded packets are computed using XOR network coding [24]. XOR network coding is a special case of linear

network coding where the coefficients $\alpha_{i,j}$ belong to $\mathbb{F}_2$. Because the coefficients are chosen between 0 and 1, the decoding procedure is much simpler. The destination nodes add the received linear combinations until they recover a single message slice. Repeating the procedure, all slices will be calculated and the original message comes out. In this work, the original message is cut into 10 slices and encoded by XOR network coding method.

In this paper, we assume that the adversary goal is to selectively drop packets in two flows, data, and ACK flows after a communication has begun in the network between a source node and the sink. We also assume that the adversary is an insider; that is, it can capture and corrupt sensor nodes, and then he launches those selective forwarding attacks from those compromised nodes. For the sake of simplicity and as previously mentioned, we distinguish these two attacks, on data and ACK flows, by naming them, respectively, *selective forwarding attack* and *flooding attack*.

Our security goal is to prevent selective forwarding attack depressing the performances of network coding. Specifically, we want to be able to preserve a high probability of successful decoding, to prevent *selective forwarding attack* and *flooding attack* from prolonging the average message decoding time, *flooding attack* from wasting the energy of the network (i.e., the energy cost must stay reasonable), preventing a network coding session from finishing (i.e., to decrease the average decoding time consumption).

3.2. Implementation Aspects. Classically, network coding is implemented using an oriented multicast as routing protocol. However, even if this method guarantees the maximum flow in the network, it is very expensive in terms of energy when considering constrained networks such as sensor networks. To preserve the diversified nature of the neighbors choice of network coding and to limit the energy consumption, we first have based all our implementations at the routing layer level and we decided to use a random version [25] of the gradient-based routing (GBR) protocol [26]—a multihop and multistream unicast routing protocol—underneath the network coding. The choice of the random GBR, as explained in [25], allows to maintain the diversified nature of the next hop neighbor required by network coding and also allows to create at the end of a multipath routing protocol useful for network coding. In all the simulations provided in this paper, we have made those implementation choices for network coding.

3.2.1. Gradient-Based Routing (GBR). GBR was first proposed in [26]. It uses a natural gradient as a metric to forward the query towards source. The metric can be regarded as physical distance, hops, or others. In this work, a query is forwarded based on the hop gradient in the sensor nodes. A node forwards the query to its neighbors including its information level about the queries. After a certain period, every sensor node builds up a *gradient table* (GTable) which indicates the distance to its sinks.

When a source node outwards a packet, it chooses a nexthop node which has the smallest gradient in GTable. Thus, each forwarder node will choose their nexthop in the same way. Finally, the path from source to sink is established ideally.

3.2.2. Random GBR. As the network coding process is only efficient if many forwarders combine/forward the encoded packets, we need to modify the original GBR proposal from single path routing to multipath routing from the source to the sink. To do so, we use [25] where the original version of GBR is randomized. This mechanism works as follows: when a source node outwards a packet, it randomly chooses a nexthop node which has a smaller gradient than him in GTable. So, at each packet sent, the choice for the source node for the next hop is randomly made leading to generate multipath routing as soon as many packets are sent which is the case for the network coding process. In the same way, each forwarder node will choose their own nexthop nodes in the same manner (at each new packet, the next hop is randomly chosen leading to create multipath when the network coding process is used). Notice that, we only allow the packets generated from the same data flow to belong to the encoding process. Each packet traversing through the network will record its path for future use because when the sink has correctly decoded the message, then it sends back through the shortest single path the ACK message. Finally, we will have multipath GBR protocol.

3.3. Our Multipath ACK Strategy against Flooding Attacks. In this section, we describe our multipath ACK scheme strategy and how we have implemented this scheme for the simulations presented in Section 4.

The algorithm we propose to prevent flooding attacks in the network is really simple.

(i) The source node Alice wants to send the data D to Bob. First, she encodes D into a certain number of m_j messages as explained in Section 2.1, and then she sends to r_1 of her neighbors the encoded packets m_j for $j = 1, \ldots$ until she receives an ACK packet.

(ii) Each of the forwarders (i.e., intermediate nodes) forwards and/or combines the received packets m_j sent by Alice to r_2 of its neighbors (note that the process for a forwarder to encode intermediate packets is the same as the one previously described) until the packets reach the sink Bob.

(iii) The sink, after having received at least n encoded packets, begins to try to decode the message D. When Bob receives a sufficient amount of data, he decodes D and sends the ACK packet through p different routes. Those p routes are selected among all the routes received by the sink: each packet m_j brings with it all the intermediate nodes from the source to the destination.

(iv) As soon as the source Alice has received one ACK packet, she stops sending combination of data of D.

The principle of this algorithm is rather simple; however, its implementation is more tricky and depends on the way

the network coding process is performed. In our case, as the network coding is implemented with the help of the random GBR protocol, we derive multipath from it for the ACK flow.

As previously defined, each sensor in the network continuously transmits encoded packets according to network coding scheme. Each encoded packet could choose several nexthop nodes by random GBR protocol. The forwarding nodes generate new encoded packets from the packets buffers and then forward to next-hops.

When the sink collects enough encoded packets of the same data flow, the data flow will be successfully decoded and recovered. Then, the sink must send back an ACK to the source to notify it to stop sending more encoded packets. Using random GBR, we can obtain several paths from the source to the sink. In random GBR, every packet records its route. So, when it arrives at the sink, the route is stored for ACK backsending. The sink maintains a routing table of distinct candidate ACK paths collected from incoming packets. Meanwhile, these paths also satisfy the condition of "the least hop counts" from the sink to the source. Therefore, the sink has many paths to send back ACK; thus the opportunity of ACK being blocked by flooding attackers is reduced.

Multipath ACK scheme is supposed to provide more opportunity to avoid the hijacking of ACK on the paths. The sink is able to choose more than one path from the candidate paths to send ACK.

4. Simulation Results without and with the Multipath ACK Strategy

In this section, we present all our simulation results concerning selective forwarding attacks and flooding attacks, first against classical network coding (without our multipath ACK strategy) and second using our solution after having shortly introduced our simulation environment.

4.1. Simulation Assumptions. All the simulations performed in this paper are carried out using the simulator WSNet [27], an event-driven network and physical layer simulator.

Our simulation results are observed in several scenarios. The result of each scenario is averaged on 20 times simulations run with n sensor nodes, where $n \in [50, 200]$ randomly distributed over a square field of 100 m by 100 m. Each sensor node has a radio range equal to 20 m. We assume that energy consumption of transmitting a packet is twice that of receiving a packet, and each sensor does not expire during the simulation duration time.

In this work, the negative influence by packet loss rate caused by signal degradation or collision in MAC layer is not taken into account, which implies that the source nodes do not retransmit the lost encoded packets but just continue sending encoding packets until the ACK arrives from the sink. The simulation duration time is 150 s. Packet transmission rate at each sensor node is one packet per second.

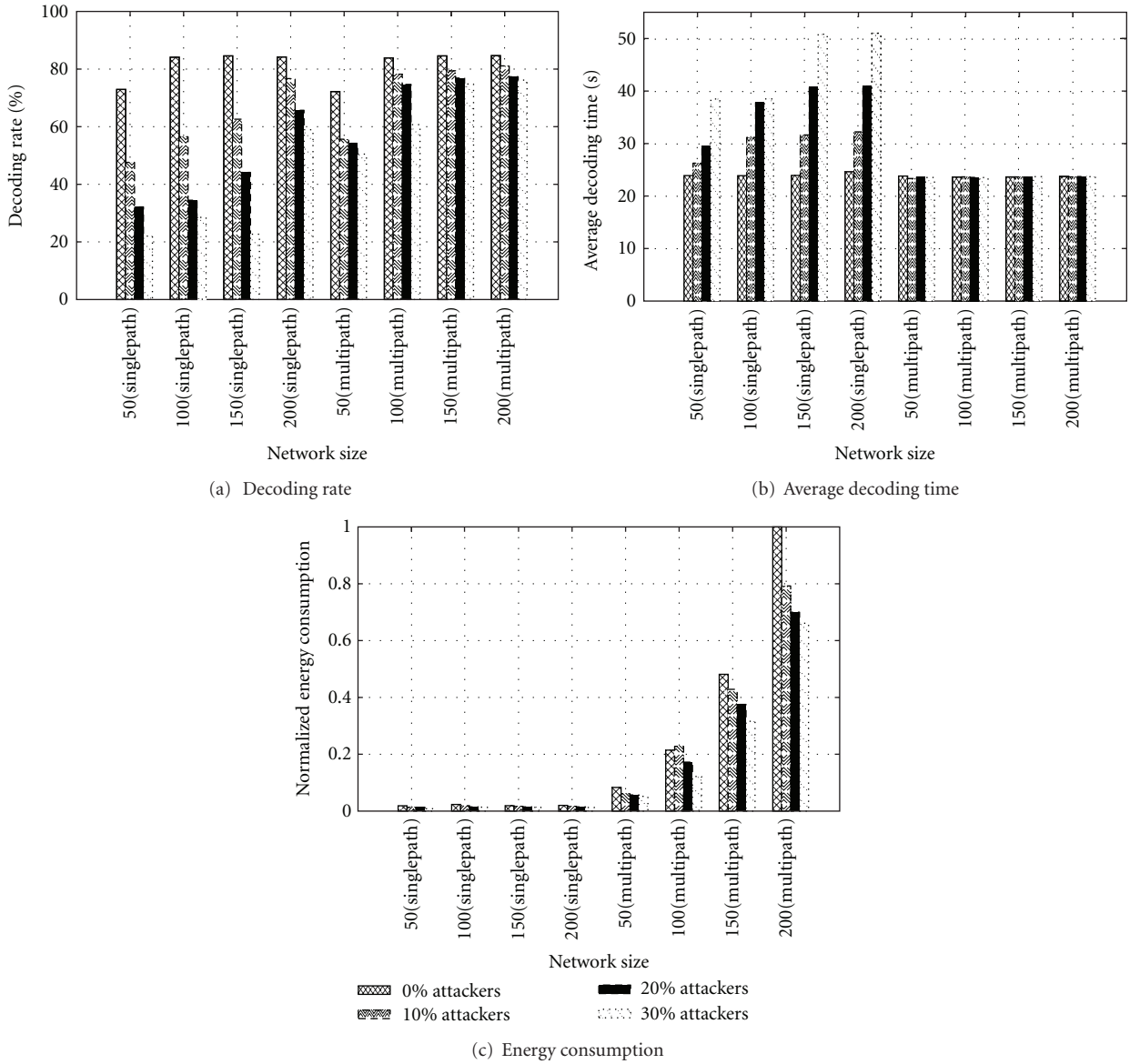
(a) Adversary Strategy. Our adversary is specialized on dropping/removing all data packets and/or all ACK packets passing through him. To do so, he compromises nodes in the network. We assume that he chooses randomly the nodes to compromise. Our adversary is not really clever in the sense that he does not take into account his position in the network. In our simulation, the number of compromised nodes is between 10% and 30% of the total.

(b) Metric. We focus essentially on evaluating the *average probability of successfully decoded messages*. This event occurs when the decoding process is successful for a given message D and when the source node stops forwarding encoded packets for this message; that is, the source receives the ACK. The *decoding rate* denotes this event, that is, the proportion of successfully decoded packets. The *average decoding time* represents the time interval, at the source node, between the moment where a raw message is generated and an ACK packet is received. The *energy consumption* represents the gain in terms of energy between the most expensive solution and the considered solution (a scale between 0 and 1).

4.2. Attacks under Study with Classical Network Coding. In this part, we give simulation results concerning the way the network coding reacts when confronting to first selective forwarding attacks and second flooding attacks when only single ACK path is considered. For comparison purpose, we also give the results for the dummy example "single path network coding strategy" which means that the network coding process works on a single path using classical GBR. In Section 4.2.1 we give the results concerning selective forwarding attacks whereas in Section 4.2.2 we give results concerning flooding attacks. In Section 4.2.3 we give the results concerning the combination of the two previous attacks.

4.2.1. Analysis for Selective Forwarding Attacks. We sum up in Figure 2 the simulation results when the network is confronted to selective forwarding attackers (from 0% to 30% of attackers), considering both network coding used with a single path (i.e., classical GBR) and network coding used with multipath (random GBR). Note that network coding with single path is only a case study which is not really interesting in concrete applications of network coding.

First, it is important to notice that the decoding rate never reaches 100% even when there is no attacker in the network. This is due to the way the simulations are processed: the simulation time is bounded and the simulations stop when the network still works. We do not wait for the successful decoding of all packets. So, all decodings are not completed; this is why the decoding rate never reaches 100%. This fact is more visible on small networks because less packets are sent in the network, leading to reduce the proportion of well-decoded packets (in the sense of our metric). Moreover, XOR network coding is not always a solution for large networks where operations on bigger finite fields are more efficient. Indeed, the number of packets that must be sent in XOR network coding must be more



(a) Decoding rate

(b) Average decoding time

(c) Energy consumption

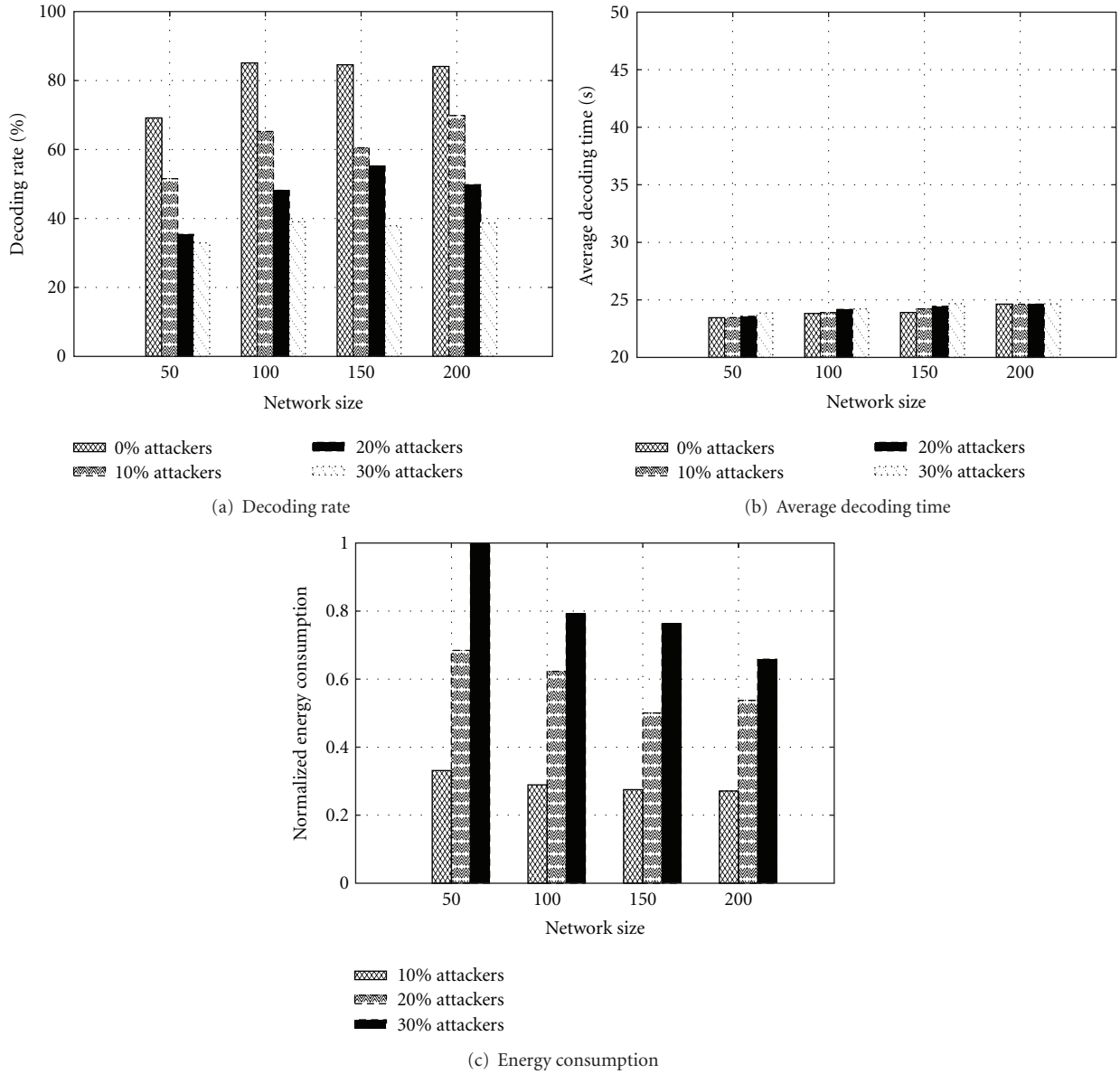
Figure 2: Performance results when single path network coding and multipath network coding are confronting to selective forwarding attackers.

important than in other cases to guarantee a correct decoding at the destination (as shown in [28]). However, we compare the different results performed in the same conditions.

So, we observe in Figure 2(a) that the decoding rate drastically decreases for the single path case when the number of attackers increases whatever the size of the network. For example, whereas the decoding rate is more than 80% when no attackers are present in a 150 nodes network, the decoding rate decreases to about 40% when 20% of the nodes are compromised and down to around 20% when 30% of the nodes are compromised. The degradation is clearly less important when the multipath strategy is used (the worst case is observed for a 50 nodes network where the decoding rate passes from 70% with 0% of attackers down to around 50% when 30% of attackers are present in the network). And larger the network is, less the degradation is important (this remark also holds for the single path case). This is due to the previous remark concerning the bounded simulation time and because, in a larger network, the opportunities of finding more paths are greater.

The average decoding times presented in Figure 2(b) clearly increase in all cases when considering single path GBR whereas the average decoding time (equal to 24 seconds) stays about the same in all cases when considering multipath scheme. This means that when multipath strategy is enabled in a sufficiently dense network, it erases all the negative effects brought by the selective forwarding attackers and makes the average time approaching the ideal value when no attackers are present in the network.

When looking at energy consumption results presented in Figure 2(c), we define the norm value equal to 1 as the biggest energy consumption which is the multipath



(a) Decoding rate

(b) Average decoding time

(c) Energy consumption

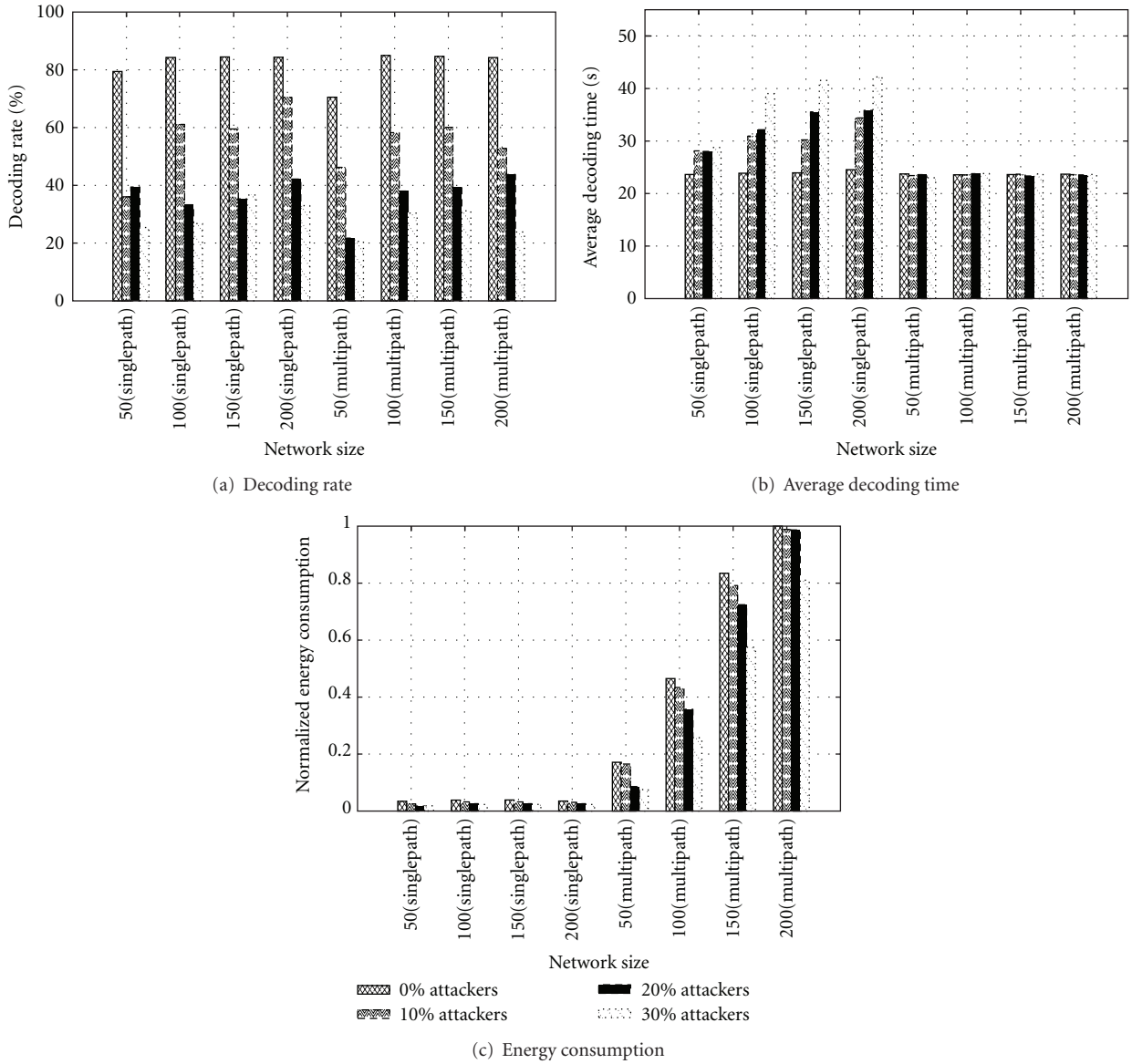
Figure 3: Performance results when multipath network coding is confronting to flooding attackers.

scenario for a 200-node network in Figure 2(c). We observe that, in single path scenarios, the energy consumption is about the same in all cases and is equal to 5% of the normalized value. This is due to the fact that the energy consumption only linearly depends on the length of the path from the source node to the sink. Moreover, in single path scenarios, the energy consumption slightly decreases when the number of attackers increases because the attackers make some packets to disappear as the energy linked with those packets. Multipath scenarios are of course much more energy consuming because several paths are in use. Moreover, bigger the network is, exponentially greater the energy consumption is. This also comes from the previous remark where the possible number of paths exponentially increases according to the size of the network.

In conclusion, we finally state that, as expected, classical multipath network coding strategies are efficient in terms of decoding rate and of average decoding time to defeat selective forwarding attackers on data flows even if the energy cost to pay can be important and even prohibitive when energy preservation is crucial for the considered network (e.g., for highly constrained networks).

4.2.2. Analysis for Flooding Attacks. As the flooding attack concerns the suppression of packets in the ACK flow, we only provide the results for the multipath scheme applied on the data flow.

As in the previous case and for the same reason, when there is no attacker in the network, the decoding rate does not reach 100%. However, concerning the decoding



(a) Decoding rate

(b) Average decoding time

(c) Energy consumption

Figure 4: Performance results when single path and multipath network coding are confronting to selective forwarding attackers and to flooding attackers.

rate, the portion of successfully decoded packets, presented in Figure 3(a), we notice a clear degradation of this rate: passing, for a 200 nodes network, from more than 80% when no attackers are present in the network to less than 40% when 30% of attackers are present. This means that many source nodes will continue to send encoded packets until they die. Thus, the success of the attacker is clear in this case.

Comparing those values with the ones of the previous section where no degradation is observed when multipath network coding is confronting to selective forwarder attackers, we deduce that flooding attack affects the network coding process in terms of decoding rate.

When looking at average decoding time shown in Figure 3(b), this value remains about the same for all cases: equal to 24 seconds. This result is exactly the same as the ones given in the previous section. This is due to the fact that the decoding time only concerns messages that have been successfully decoded, that is, messages that have been correctly sent and where the ACK has been correctly received by the source node. In other words, this value only concerns messages that have not encountered any attacker. So, this value remains normally the same.

When ACK is hijacked by flooding attackers, even after the successful decoding process at the sink, the source node continues sending encoded packets, and others receive and forward these packets. *Energy consumption* measured in this section is the sum of these extra consumptions. Scenario with a 50-node network fronting 30% attackers is used as the norm value, and the others are normalized according to this norm, as shown in Figure 3(c). The results concerning the

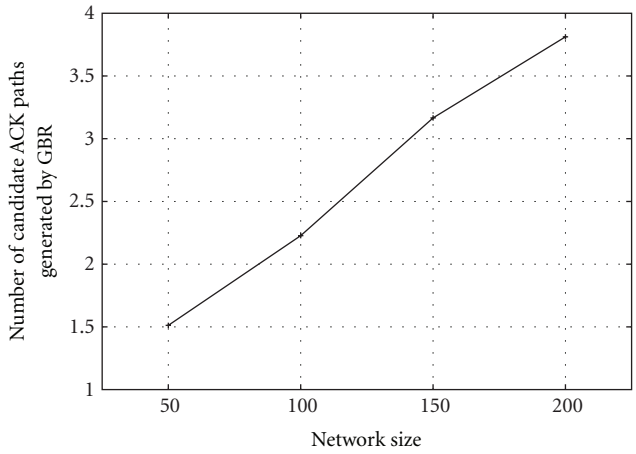


Figure 5: Evolution of the average number of ACK paths generated by GBR as a function of the network size.

case of 0% attackers do not appear on Figure 3(c) because they are all too close to 0. So, the most expensive case is the 50-node network with 30% of attackers. It means that the energy wasted in the network due to the absence of ACK back is huge. The results for 30% of attackers and other network sizes proportionally imply less degradation because the diversity of possible ACK paths is more important leading to waste less energy due to source nodes that continue to send packets. In the same way, with fewer attackers present in the network (10% and 20%), the energy waste is less important because more ACK messages reach their destinations.

In conclusion, and as observed in our simulations, the flooding attack is clearly an efficient attack against the network coding process because network coding does not provide intrinsic mechanisms to prevent attacks against the ACK flow. This is why we propose such a mechanism in our paper.

4.2.3. Analysis for Combining Attacks. A critical question for network coding security is to combine all the solutions dedicated to a given attack and to evaluate the performances in the presence of all kind of adversaries. Our results include both selective forwarding attacks on the data flow and flooding attacks. Those results are presented in Figure 4: the percentage x% of compromised nodes corresponds to x% of flooding nodes on the ACK flow and of x% of selective forwarding nodes in the data flow.

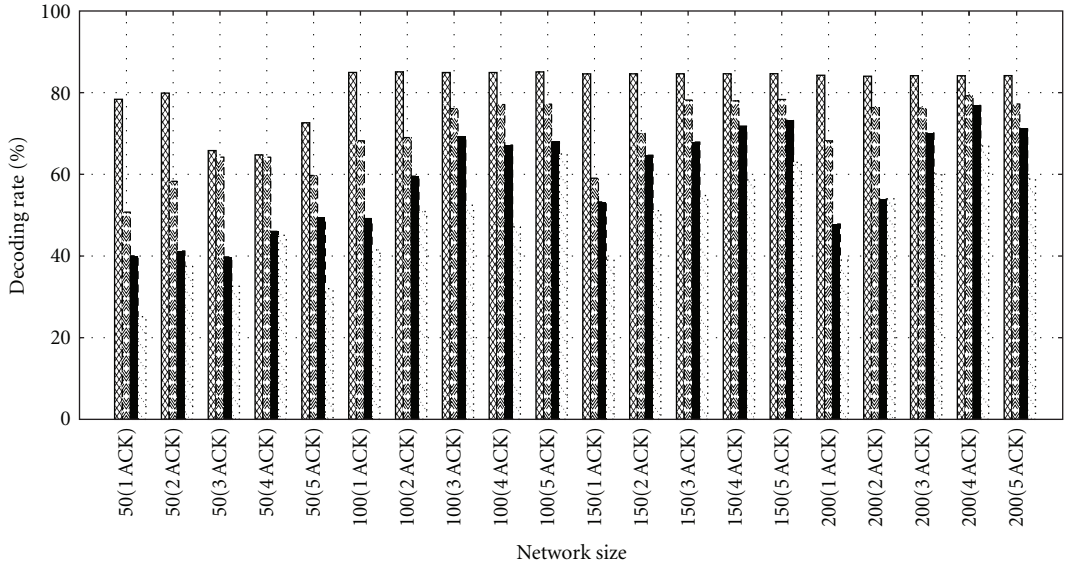
As in Section 4.2.1, we present the results for the dummy example "network coding with single path and single ACK back path" for comparison purpose. In Figure 4(a), we observe that the decoding rate, with respect to the number of attackers, always degrades for all the network sizes and all the strategies. The degradation for the single path strategy comes essentially from the selective forwarding attackers even if the presence of flooding attackers increases the degradation (when compared with Figure 2(a)). Figure 4(a) exactly reflects the severe impact of the flooding attack on the network. The influence is so significant that it overwhelms all the advantages brought by multipath data forwarding. As we can see in Figure 2(a), the multipath data forwarding method is applied against selective forwarding attacks, so the performance results of 10%, 20%, and 30% attackers are close to the ones with 0% attackers. We assume that the multipath method almost compensates all the negative influences from selective forwarding attacks. And we release two attacks in Figure 4(a) scenario: the selective forwarding attack and the flooding attack. The selective forwarding attacks impose great performance degradation onto the data flow from the source to the sink, but the multipath data forwarding method helps the network to overcome the performance loss, according to Figure 2(a). The flooding attacks impose performance degradation on the ACK flow. It is obvious that the performances brought down by flooding attacks are dominant in this scenario. That means that the advantages of multipath data forwarding strategy are totally overwhelmed by the flooding attacks.

Concerning the average decoding time presented in Figure 4(b), surprisingly, the times for the single path strategies are better than the ones in Figure 2(b) for all network sizes. This is due to the fact that less packets arrive at the sink, and less ACKs are returned to the source nodes. So, messages that are correctly decoded are less numerous and require less time to be correctly decoded. As already observed in Figures 2(b) and 4(b), in the case of multipath strategies, there is no significant degradation of decoding time for the same reasons as the ones exposed in Sections 4.2.1 and 4.2.2 This essentially comes from the fact that the decoding time only concerns packets well received at the sink and well acknowledged at the source nodes.

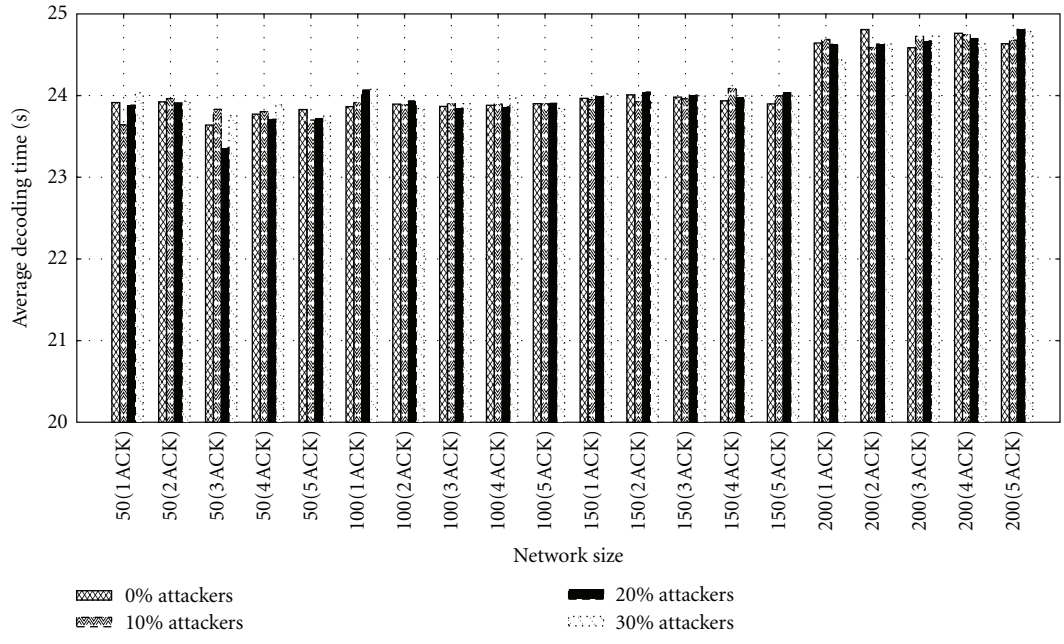
In Figure 4(c), we observe the energy consumption results where the norm value is for 0% attackers, a network with 200 nodes and multipath network coding as in the case of Figure 2(c). Anyway, Figures 4(c) and 2(c) have the same main characteristics. However, the energy consumption for multipath strategies is worst in all cases when both attacks are combined due to the flooding attacks effect. For single path strategies, surprisingly the energy consumption is about the same proportion as in Figure 2(c) (the values are also about to be the same). These surprising results come from the combining effects of flooding attacks that discard the acknowledgements and make the source nodes to continue to send packets and effects of selective forwarding attacks that discard a part of those exceeded packets sent. More generally, the energy consumption of the single path strategies is small when compared with all multipath strategies.

When combining both attacks, clearly the simulation results also combine the worst performances of each attack so the decoding rate for single path strategies has about the same behavior (in worst) as in the case of selective forwarding attackers whereas the decoding rate and the decoding time for multipath strategies have about the same behavior (in worst) as in the case of flooding attackers.

4.3. Attacks under Study with Multipath ACK Network Coding Strategy. In this part, we sum up our simulation results and the corresponding analysis when our multipath ACK network coding strategy is used in the network. All simulations are performed using the same experimental



(a) Decoding rates



(b) Decoding times

Figure 6: Decoding rates and decoding times when network coding is confronting with flooding attackers.

conditions and the same metrics than the ones described in Section 3. We first study the evolution of the number of paths available in the network to send back the ACK, as this parameter is critical in our problem.

4.3.1. Average Number of Paths from Random GBR. As explained in Section 3.3, the successful transmission of the ACK depends essentially on the capabilities and the opportunity to send back the ACK packets to the source node. Intuitively, it should be accomplished by using as many paths as possible. In fact, the ideal number of ACK paths is not "the bigger the better," as this will be bounded by the routing protocol parameters. Our simulation results show, in Figure 5, that, for GBR and for the network sizes considered here, the average number of established ACK paths is always less than 4.

This average value becomes constant as the network grows as shown by other simulations not drawn in Figure 5 where a clear logarithmic effect appears. So in this case, it however remains better to use 4 or 5 paths to send back ACK packets rather than 2 or 3. Those results can also be seen in Figure 6(a).

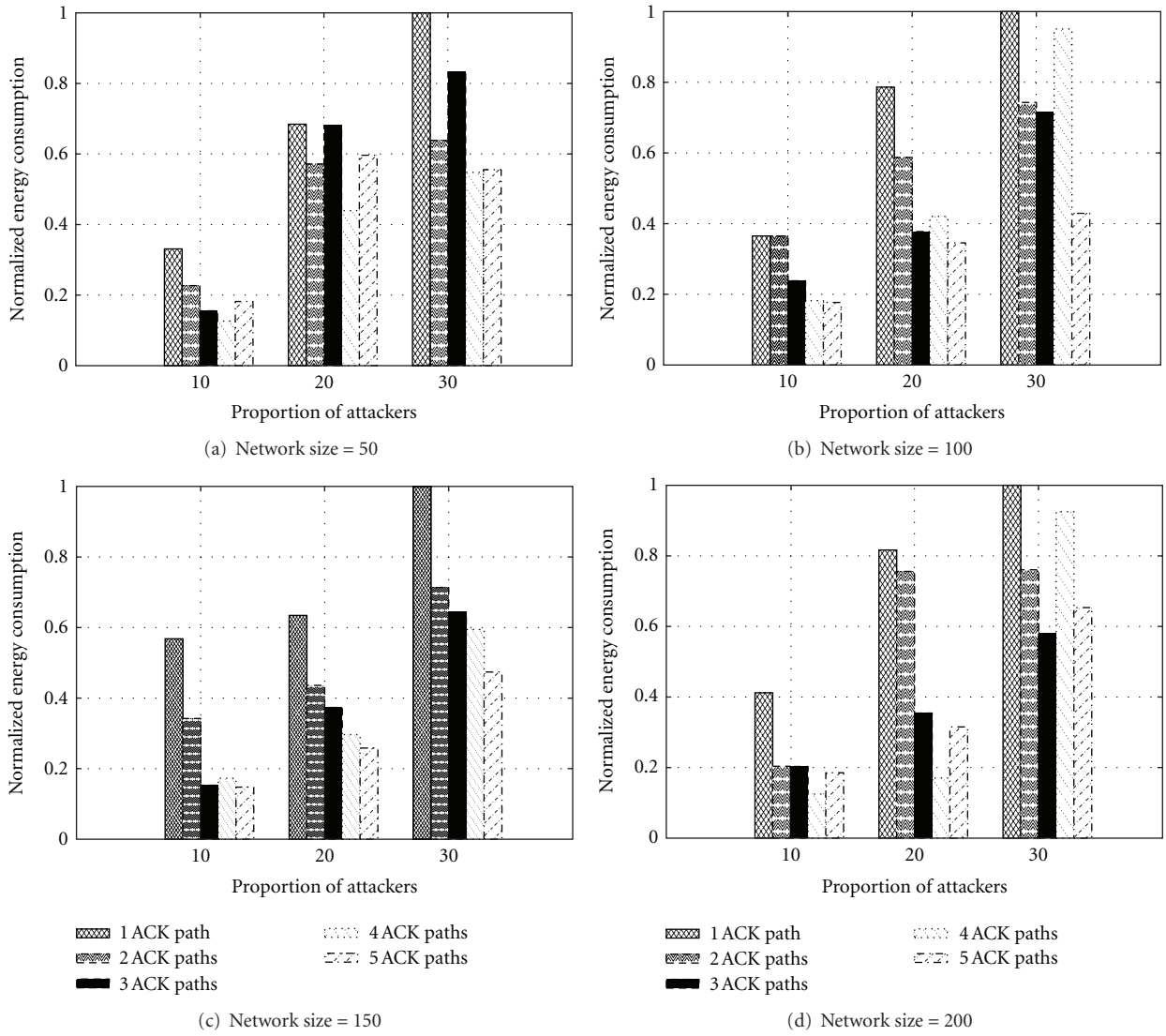
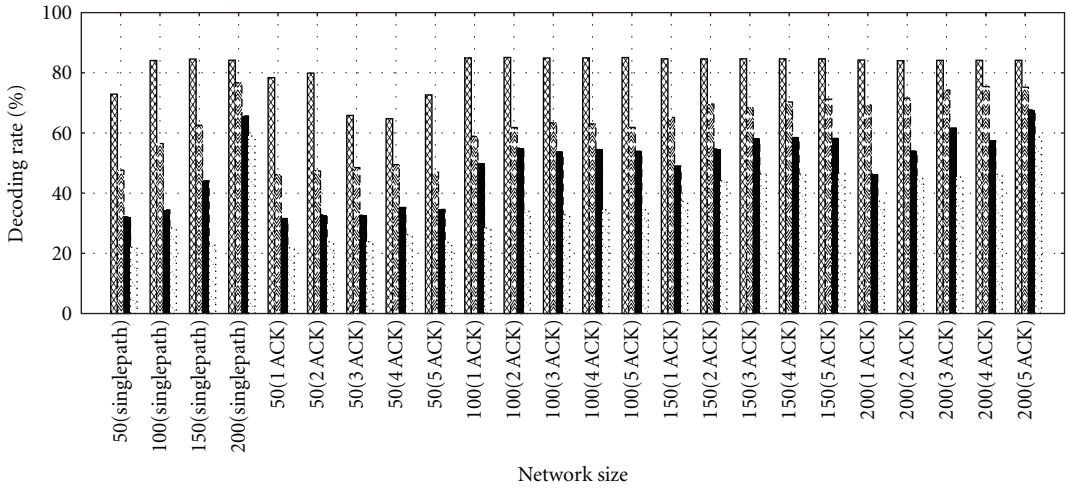


Figure 7: Extra energy consumption *when network coding is confronting with flooding attackers *when ACK is intercepted, the source node still sends encoded packets. The sending and receiving of these packets cause extra energy consumption. *Refers to all figures presesnted in this figure.

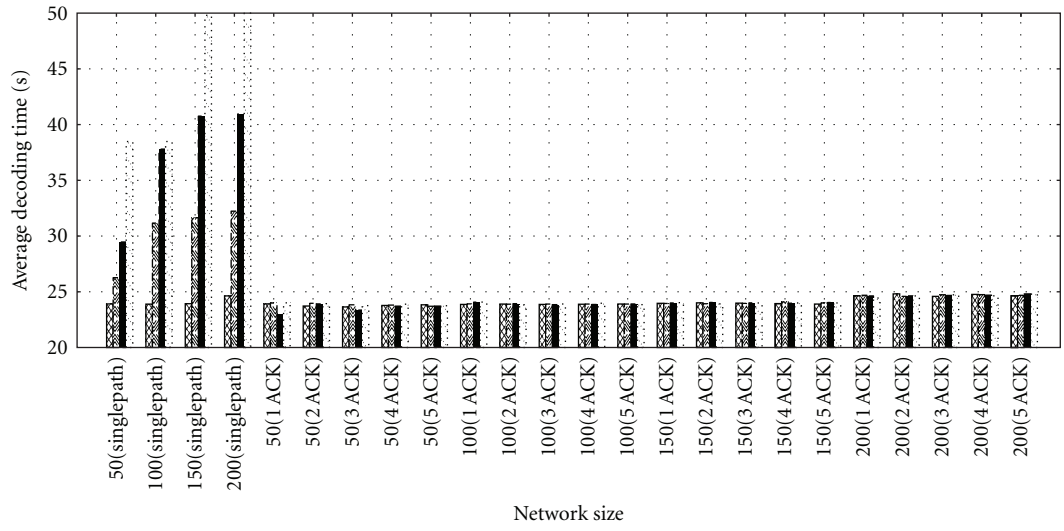
4.3.2. Results Concerning Flooding Attackers. The results in Figure 6(a) also show that even if our multipath ACK strategy is not so efficient in small networks, it becomes interesting (increasing the rate of successfully decoded packets) as soon as the network is sufficiently large, that is, dense. For example, for 5 ACK and 200 nodes, the decoding rate is equal to 79% when 10% of attackers are present into the network and decreases to 62% when 30% of nodes are malicious which gives better rates and better digressions than with only one ACK path.

The results are more significant in larger networks because smaller networks have fewer paths (as shown in Figure 5) available for the sink to send back ACK packets. Therefore, multipath ACK strategy is much more suitable for networks with larger size, that is, dense networks. On the other side, we should notice that using more ACK paths does not always help improving the performances, as we already explained in Section 4.3.1 and as shown in Figure 6(a). We can see in every figure that the performance gap among scenarios with one ACK path, two ACK paths, and three ACK paths is larger than others; that is, the number of packets successfully decoded in scenarios with two ACK paths and three ACK paths is 28% and 47% more than for the scenario with one ACK path approximately, while scenarios with four and five ACK paths have improvements of 45% and 53%, respectively. Employing many ACK paths is interesting only when numerous paths are available which is not always the case even for dense networks as shown in Section 4.3.1.

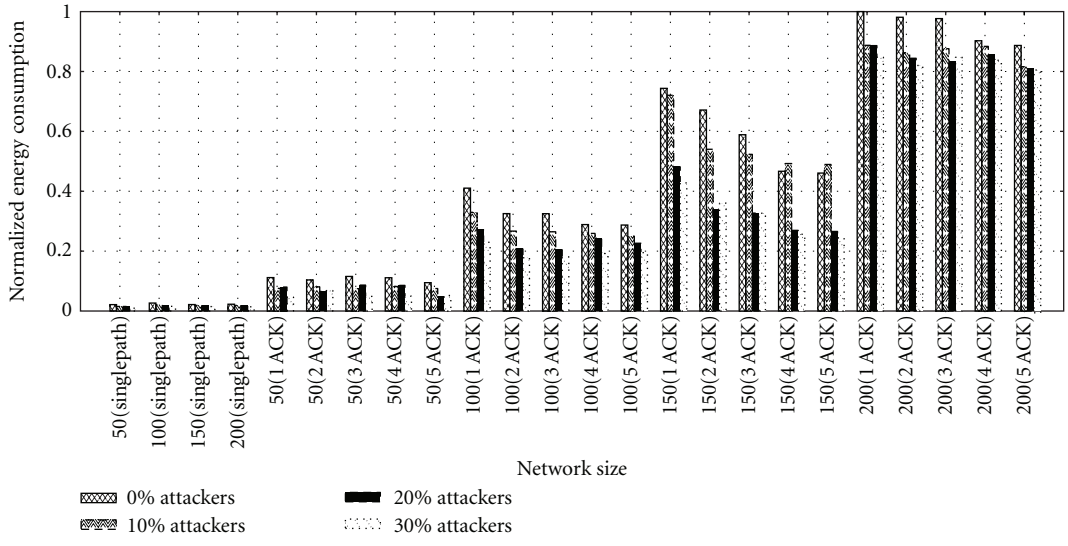
The worst case possible scenario to occur is when attackers are inserted on all different paths between the sink and the source node. This can happen when we deal with very clever attackers (this is not the case here where the attackers are randomly picked among all the nodes). Those particular attackers have an excellent analysis of the network traffic. However, our proposal stays efficient because the routes are at each time taken as random (due to the design of



(a) Decoding rates



(b) Decoding times



(c) Energy consumptions

Figure 8: Combined flooding and selective forwarding attackers: comparison of the number of decoding rates, decoding times, and energy consumptions in case of 1 ACK path, 2 ACK paths, 3 ACK paths, 4 ACK paths, and 5 ACK paths.

the random GBR protocol described in Section 3.2.2) where an attacker could not know all the random routes used by the encoded packets from a source to the destination as explained in [25].

In Figure 6(b), we present the results concerning the average decoding time. This time stays about the same in all cases even if the cases with 4 and 5 ACK paths seem to give the best decoding time. In all cases, the values observed stay around 24 seconds and do not seem to generate a big degradation of performances. However, the decoding time for a 200 nodes network is a little bit greater due to the size of the network. We have implemented the same scenario with bigger network sizes and have noted that the decoding time growth steepens from network size 200 and above.

In Figure 7, we present the results concerning energy consumption gain. When ACK flow is hijacked by flooding attackers, even after the successful decoding process at the sink, the source node continues sending encoded packets, and others receive and forward these packets. Figure 7 highlights those extra consumptions. The norm value of our figures equal to 1 (which is the most energy consuming one) is for each network size, the energy consumed when 30% of attackers are present in the network and when only one ACK path is used. This corresponds with the case where the most of energy is dissipated in the network due to the source nodes that continue to send encoded packets as already mentioned.

It is interesting to notice here that even if multiplying the ACK paths consumes energy, this consumption is marginal when compared to the flooding provoked by the disappearance of the ACK packets. So, in terms of energy consumption, our multipath ACK solution is really efficient when compared with the single ACK path (e.g., when 30% attackers are present in the network, 5 ACK paths solution only consumes half of the energy of the 1 ACK path solution). Indeed, with only one ACK path, the probability that the ACK packets are thwarted by the attackers is high; thus the source and intermediate nodes continue sending and forwarding packets, which is exactly the cause of unnecessary energy waste.

4.3.3. Results When Combining Selective Forwarding Attackers and Flooding Attackers. As already mentioned in Section 4, it is really important when a security solution is proposed to combine possible attacks and to evaluate the performances in the presence of all kinds of adversaries. The results presented in this section include both selective forwarding attacks on the data flows and flooding attacks. Those results are presented in Figure 8: as previously, the percentage x% of compromised nodes corresponds to x% of flooding nodes on the ACK flow and of x% of selective forwarding nodes in the data flow.

When we bring two attacks into the network, as shown in Figure 8, the performances of single path scenarios do not vary from results of Figure 4. When we switch on the multipath option, *average decoding time* keeps up with the good results of Figures 2(b) and 6(b), but *decoding rate* has been drawn back by flooding attackers. Because the attacks take effects on different flows, analysis on separated attacks is much more effective and clearer to unveil the advantages brought about by multipath method.

All the results presented in Figure 8 are always worse than those presented in Figures 6 and 7. This comes from the fact that selective forwarding attackers on the data flows introduce a delay for a correct decoding of the packets, and as the simulations made here hold the same time in all cases, the portion of correctly decoded packets is worse. Those effects are less significant for larger networks because the delay induced by selective forwarding is less important. Note also that for dense networks our multipath ACK strategy against flooding attackers stays efficient.

This combined attacks scenario also highlights the fact that our strategy is more efficient in cases of dense networks as shown in Figure 8(a). Moreover and as expected, the impact of selective forwarding is not efficient due to the intrinsic nature of the network coding.

5. Conclusion

We have considered selective forwarding attacks against both data flows and ACK flows in network coding applications. The impact of those attacks has been studied when the adversary randomly compromised the nodes.

Due to its intrinsic multipath nature, network coding is resilient against selective forwarding attackers even if this kind of attacks introduces a little delay in the network. This is the first step we want to demonstrate in this paper. We do not develop here a dedicated mechanism to identify and avoid attackers in the network because we only want simple mechanisms that could be added to the routing layer complementary with network coding to bypass the attackers at a reasonable cost.

Against flooding attacks, our countermeasure is based on multipath ACK, and it is a randomized variant of GBR that allows to build several backward paths we use for the ACK sent. Our simulation results have shown that our solution is efficient as soon as we have a sufficient number of distinct backward paths. Such condition is easily obtained in dense networks.

The choice of the routing protocol is critical, and the key feature is the capacity to generate randomly many paths: greater are the paths of the ACK, higher is the probability to thwart flooding attacks.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (no. 61103040).

References

[1] L. Lima, J. Barros, and M. Médard, "Random linear network coding: a free cypher?" in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '07)*, pp. 176–180, Nice, France, July 2007.

[2] N. Cai and R. W. Yeung, "Secure network coding," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '02)*, p. 323, July 2002.

[3] S. Y. El Rouayheb and E. Soljanin, "On Wiretap networks II," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '07)*, pp. 551–555, Nice, France, June 2007.

[4] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient scheme for securing XOR network coding against pollution attacks," in *Proceedings of the 28th IEEE Communications Society Conference on Computer Communications (IEEE INFOCOM '09)*, pp. 406–414, Rio de Janeiro, Brazil, April 2009.

[5] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient signature-based scheme for securing network coding against pollution attacks," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (IEEE INFOCOM '08)*, pp. 2083–2091, Phoenix, Ariz, USA, April 2008.

[6] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks," in *Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec '09)*, pp. 111–122, ACM, March 2009.

[7] A. Apavatjrut, W. Znaidi, A. Fraboulet, C. Goursaud, C. Lauradoux, and M. Minier, "Energy friendly integrity for network coding in wireless sensor networks," in *Proceedings of the 4th International Conference on Network and System Security (NSS '10)*, pp. 223–230, IEEE, September 2010.

[8] D. Charles, K. Jain, and K. Lauter, "Signatures for network coding," *International Journal in Information and Coding Theory*, vol. 1, no. 1, pp. 3–14, 2009.

[9] D. Boneh, D. Freeman, J. Katz, and B. Waters, "Signing a linear subspace: signature schemes for network coding," in *Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography (PKC '09)*, vol. 5443 of *Lecture Notes in Computer Science*, pp. 68–87, Springer, Irvine, Calif, USA, 2009.

[10] S. Agrawal and D. Boneh, "Homomorphic MACs: MAC-based integrity for network coding," in *Proceedings of the 7th International Conference on Applied Cryptography and Network Security (ACNS '09)*, vol. 5536 of *Lecture Notes in Computer Science*, pp. 292–305, Paris, France, 2009.

[11] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Secure network coding for wireless mesh networks: threats, challenges, and directions," *Computer Communications*, vol. 32, no. 17, pp. 1790–1801, 2009.

[12] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on TCP," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 208–223, IEEE Computer Society, Oakland, Calif, USA, May 1997.

[13] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[14] T. Ho and D. Lun, *Network Coding: an Introduction*, Cambridge University Press, 2008.

[15] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, *Network Coding Theory*, NOW Publishers, 2005.

[16] J. Cannons, R. Dougherty, C. Freiling, and K. Zeger, "Network routing capacity," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 777–788, 2006.

[17] T. Ho, M. Médard, R. Koetter et al., "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[18] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[19] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 255–265, ACM, Boston, Mass, USA, August 2000.

[20] H. Krawczyk, "LFSR-based hashing and authentication," in *Proceedings of the Annual International Cryptology Conference (CRYPTO '94)*, vol. 839 of *Lecture Notes in Computer Science*, pp. 129–139, Springer, Santa Barbara, Calif, USA, 1994.

[21] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," 1997, rFC 2104.

[22] J. Black and P. Rogaway, "CBC MACs for arbitrary-length messages: the three-key constructions," *Journal of Cryptology*, vol. 18, no. 2, pp. 111–131, 2005.

[23] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02)*, pp. 41–47, ACM, Washington, DC, USA, November 2002.

[24] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "XORs in the air: practical wireless network coding," *IEEE/ACM Transactions on Networking*, vol. 16, no. 3, pp. 497–510, 2008.

[25] O. Erdene-Ochir, M. Minier, F. Valois, and A. Kountouris, "Toward resilient routing in wireless sensor networks: gradient-based routing in focus," in *Proceedings of the 4th International Conference on Sensor Technologies and Applications (SENSORCOMM '10)*, pp. 478–483, Venice, Italy, July 2010.

[26] J. Faruque and A. Helmy, "Gradient-based routing in sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 4, pp. 50–52, 2003.

[27] A. Fraboulet, G. Chelius, and E. Fleury, "Worldsens: development and prototyping tools for application specific wireless sensors networks," in *Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN '07)*, pp. 176–185, ACM, April 2007.

[28] M. Médard and R. Koetter, "Beyond routing: an algebraic approach to network coding," in *Proceedings of the IEEE Communications Society Conference on Computer Communications (IEEE INFOCOM '02)*, pp. 122–130, IEEE, New York, NY, USA, June 2002.