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