2012 IEEE ESTEL Conference

Interoperability Solutions Between Smartphones and Wireless Sensor Networks

Mauro De Sanctis, Cosimo Stallo, Stefano Parracino, Marina Ruggieri, Ramjee Prasad
University of Rome Tor Vergata, viale del Politecnico 1, 00133 Rome, Italy
mauro.de.sanctis@uniroma2.it

***Abstract*— The work aims at discussing possible engineering solutions to guarantee the interoperability between smartphones and WSN under high mobility levels. The paper discusses an application scenario where some of the most interesting standards for WSNs can be effectively employed together with smartphones. The architectures supporting interoperable smartphone/WSN systems, considering network topology and functionalities of the nodes are presented together with current network solutions for interoperability.**

***Index Terms*—Wireless Sensor Networks, DASH7, 6LOWPAN, Interoperability.**

I. Introduction

THE interoperability between smartphones and Wireless Sensor Networks (WSNs) is an interesting engineering problem which is worth of consideration, accounting for the wide set of applications that can cover.

We refer to a smartphone as a mobile device with powerful computing capabilities and an operating system supporting advanced user applications. A smartphone is provided with several air interfaces for voice, video and data communication such as UMTS, Bluetooth (BT), WiFi, and several internal sensors such as gyroscope, accelerometer, magnetometer and Global Positioning System (GPS) receiver. Currently, commercial smartphones are not provided with air interfaces for direct communication with external sensors. In fact, there are many different technologies for WSNs (not including BT which is not suitable for WSNs) and it is not easy to choose the best one for all possible applications. Furthermore, the WSNs can be integrated with active devices, namely actuators, to form a Wireless Sensor and Actuator Network (WSAN), or can include Radio Frequency Identification (RFID) systems, thus expanding the set of applications. This integrated view is an example of realization of the paradigm known as “Internet of Things”.

In literature, there are few examples of interoperability between smartphones and WSNs, but no flexible and complete solution is provided. The work presented in [1] focuses on using smartphones to collect data from sensor nodes opportunistically. In [2], authors have shown a novel smartphone application for personal surveillance using camera sensor networks. The interoperability is achieved through a server which is connected to the smartphone via a WiFi wireless network and the WSN are connected to the server via a USB mote. An example of convergence between WSNs, WiFi and long range wireless networks (3G) in a single smart device has been provided in [3] for the special case of emergency management systems. Authors of [4] have proposed a system consisting of Crossbow IRIS on-body sensor motes and a TelosB base station connected to an Android smartphone via USB.

A solution example is presented in [5] where an intermediate mobile device, with both BT and Xbee transceiver modules, has been used for the communication among Xbee sensors and a BT enabled smartphone. In [6], different possibilities to interconnect wireless sensor nodes and smartphones has been analysed in the context of transport processes employing road transportation with trucks.

In the paper we aim at discussing possible engineering solutions to guarantee the interoperability between smartphones and WSN. The paper is organized as follows. Section II discusses an application suitable for the considered scenario. Section III reviews some of the most interesting standards for WSNs. Section IV discusses the architectures supporting interoperable smartphone/WSN systems considering network topology and functionalities of the nodes. Section V presents current network solutions for interoperability, while conclusions are provided in Section VI.

II. Application Scenarios

In the following we show an interesting application scenario, namely safety at work, which effectively exploits a technological platform based on the interoperability of smartphones and WSNs.

In a safety at work scenario, where workers are placed in a hazardous environment, risk prevention is based on the platform's ability to detect critical situations (for example, access to dangerous areas, lack of protections of the worker, etc.) and the ability to trigger alarms (see Figure 1). We assume that every worker is equipped with an RFID for identification purposes. In addition, each wearable protection may include a sensor that notifies if the protection is correctly worn or not. Access to certain areas may be restricted to authorised employees or to workers who wear their helmet. However, the access policy can be changed by the safety management center/responsible. In a scenario of safety at work for a generic industry, the mobile elements are represented by

978-1-4673-4688-7/12/$31.00 ©2012 IEEE

workers and the objects they use as hammers, excavators, etc. Mobility cannot be determined a priori, and in any case can be highly variable (from pedestrian to vehicular).

A platform for safety management at work includes a subset of the following technologies:

- sensors inserted in the protective equipments of workers with the aim to determine their proper use. Wearable protective equipments include helmets, safety shoes, goggles, respirators, harnesses, fireproof suits. For example, a sensor on a safety helmet can notify through a wireless sensor network when the helmet is properly worn by the worker;
- sensors included in environmental protection elements with the aim to determine their position. The elements of environmental protection usually include fire doors and fire extinguishers;
- sensors included on special machines that can be used only by qualified personnel (previously identified) and only for a certain period of time;
- infrastructure sensors able to detect risk factors in the work areas, e.g. exceedance of minimum or maximum of some parameters such as temperature and content of oxygen or toxic gases in the air;
- wearable sensors that detect risk factors directly from the worker. They can be biomedical sensors (heart rate, oxygen saturation), sensors of mechanical stress (vibration, falls), or ones that measure parameters of the environment surrounding the worker (radiation, temperature, air quality);
- actuators that allow you to change the environment surrounding the individual worker. They include portable display (for images and video), loudspeakers, vibrating motors, etc.
- actuators that allow to modify the conditions of the work areas. They include sirens, automatic door locks and displays;
- access control systems for special work areas that are separated by physical or logic barriers. This system can allow or deny access to certain areas based on the identity of the person, his status and protections he/she warns;
- a system for tracking the position of workers;
- a system for the control of competitive activities;
- a control system interoperable with labor inspectors.

III. Selection of Standards for Wireless Sensor Networks

Among many wireless sensor networks, the most promising ones are two: 6LoWPAN and DASH7.

A. 6LoWPAN

6LoWPAN (*Low power Wireless Personal Area Networks*) concept is originated from the idea that low-power devices with limited processing capabilities should be included in the Internet of Things [7]. 6LoWPAN presents an adaptation layer among the IP (Internet Protocol) stack's link and network layers to enable efficient transmission of IPv6 datagrams over 802.15.4 links, drastically reducing IP overhead.

The adaptation layer provides both header compression to reduce transmission overhead, and fragmentation to support the IPv6 minimum maximum transmission unit requirement.

6LoWPAN achieves low overhead by coupling traditional protocol layers. Moreover, it uses information in the link and adaptation layers to compress network and transport layer headers. Drawing on IPv6 ex-tension headers, it employs the header stacking principle to separate orthogonal concepts and keep the header small and easy to parse.

The 6LoWPAN format defines how IPv6 communication is carried in 802.15.4 frames and specifies the adaptation layer's key elements. 6LoWPAN has three primary elements:

1. Header compression. IPv6 header fields are eliminated from a packet when the adaptation layer can derive them from the link-level information carried in the 802.15.4 frame.
2. Fragmentation. IPv6 packets are fragmented into multiple link-level frames to accommodate the IPv6 minimum MTU (Maximum Transmission Unit) requirement.
3. Layer-two forwarding: the adaptation layer can carry link-level addresses for the ends of an IP hop. Alternatively, the IP stack might accomplish intra-PAN routing via layer-three forwarding, in which each 802.15.4 radio hop is an IP hop.

B. DASH7

DASH7 (*Developers' Alliance for Standards Harmonization of ISO 18000-7*) [8] wireless sensor network uses the 433.92 MHz frequency, which is available and license-free.

That frequency range is ideal for wireless sensor networking applications since it penetrates concrete and water, but also is able to transmit/receive over very long ranges without requiring a large power draw on a battery. The low input current of typical tag configurations allows for battery powering on coin cell or thin film batteries for up to 10 years.

Unlike most active RFID technologies, DASH7 wireless sensor network supports tag-to-tag communications which, combined with the long range and signal propagation benefits of 433 MHz, makes it an easy substitute for most wireless "mesh" sensor networking technologies. DASH7 wireless sensor network also supports data encryption/decryption and IPv6 (Internet Protocol Version 6) [9].

DASH7 has been designed to operate using the "BLAST" concept: *Bursty*, *Light-data*, *ASynchronous*, *Transitive* [9].

- Bursty: data transfer does not include content such as video or audio;
- Light-data: packet sizes are limited to 256 bytes in conventional applications;
- Asynchronous: its main method of communication is by command-response, which requires no synchronisation among devices;

- Transitive: a DASH7 system is inherently mobile. Unlike other wireless technologies, it is upload-centric, so devices do not have to be to be managed extensively by a base station.

The ISO 18000-7:2004 establishes physical and data link layers. The physical layer defines the modulation used in air communications and band frequencies. The data link layer defines the communications protocol, data header, commands, data, collision treatment, broadcast communication and point-to-point communication.

The DASH7 network topology is based on master-slave mode, also called interrogator and tag. The interrogator asks the tags to collect their IDs by broadcast and it sets a Window Size (WS) in number of slots. The slot during which to transmit is chosen randomly by the tag. In case of collision between tags, they choose another random slot to transmit (Slotted Aloha Method). After WS slots the interrogator sends a sleep signal to the tags who answered the first collection round, and then it starts again another collection round, until there is no more answer.

Moreover, the interrogator can encrypt the connection between the tag by setting a password. To allow a new password, the tag must be unlocked first with the old password. Tags are unlocked by default. Locked tags answer a point-to-point communication only if the message is encrypted with this password, but broadcast message are not affected by locked or unlocked status. DASH7 mode 2 can use AES (Advanced Encryption Standard) public key.

Table 1 shows performance comparison of DASH7 and other communication protocols for wireless sensor networks.

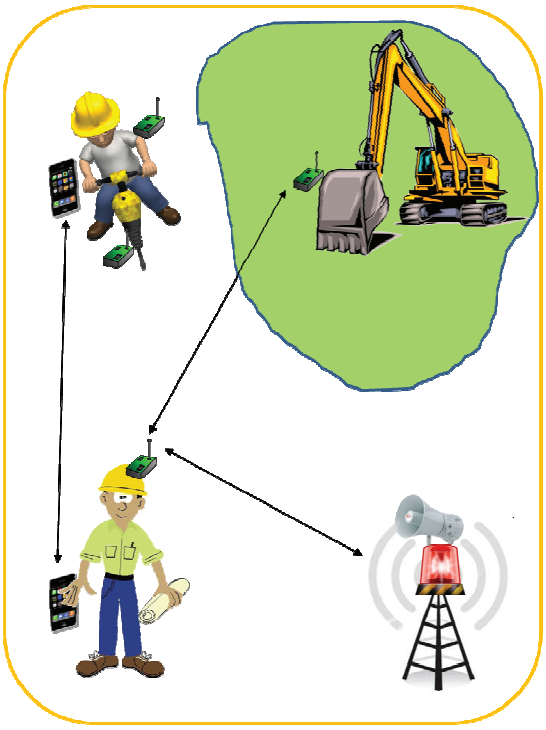

Figure 1: Pictorial view of a technological platform based on the interoperability of smartphones and WSNs for the management of safety at work.

IV. Architectures for Interoperability

The Section presents a system architecture including network topology and node functionalities which is the basis of interoperability solutions between smartphones and WSNs. The architecture allows to exchange data from a source of information to a destination.

Typical sources of information include sensors, databases (record retrieval) and application-level user interfaces with input capabilities, while typical destinations of information include actuators, databases (record insertion) and application-level user interfaces with output capabilities.

Interoperability solutions between different wireless network standards (e.g. 3G/UMTS and WSN/6LoWPAN) are based on the use of one or more multi-radio nodes which allows the simultaneous operation of different transceivers.

The architecture include several nodes with different functionalities: the sink, the gateway, the cluster head, the base station. The base station is the fixed node which allows data communication of the smartphone through Internet. The sink node is a special node of a WSN which function is to gather the collected data and send it outside the network.

A WSN can include more than one sink and the displacement of sinks can be planned through a complex optimization problem. Node clustering is a popular technique to reduce energy consumption in large scale WSNs.

A cluster is a group of nodes (usually covering a convex area) coordinated by a cluster-head node which is responsible to gather data from sensor and to send data to the sink. Data delivery from the cluster-head to the sink can be achieved through a direct single hop link or through an indirect multiple hop path using other cluster heads of the WSN.

The gateway node is the entry/exit point between the two networks, i.e. 3G/UMTS and WSN/6LoWPAN.

The gateway node is responsible for protocol translation thus permitting the communication between network based on different standards/protocols.

Depending on the hierarchical organization of the WSN, cluster-head, gateway and sink functionalities can be referred to the same node. Since the aim of the architecture is to allow interoperability between a smartphone and a WSN, we do not deal with the sink and cluster-head functionalities, but we focus on the gateway.

The architecture can be structured through two different interoperability solutions:

- *Direct Interoperability*: the smartphone is physically connected with the WSN sink/gateway node (i.e. through a wired connection integrated within the smartphone or through a USB dongle). This architecture solution exploits a single gateway, i.e. the smartphone (see Figure 2).
- *Indirect Interoperability*: the smartphone is wireless connected with the WSN sink/gateway node (i.e. through a BT or WiFi link). This architecture solution exploits two multi-radio gateways: the smartphone and the the gateway BT/WSN (see Figure 2).

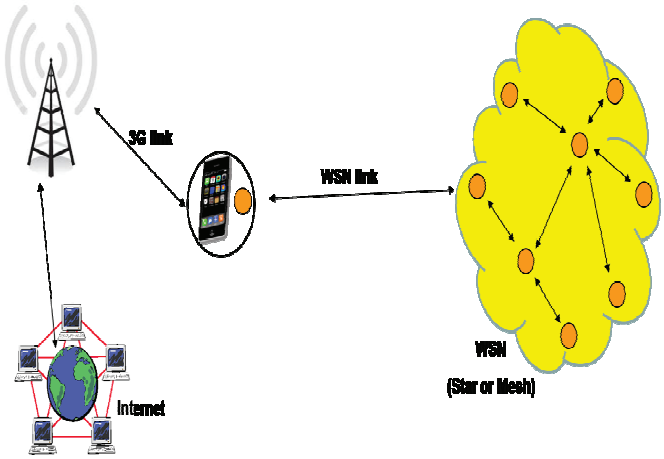

Figure 2: Architecture for direct interoperability between a smartphone and a WSN.

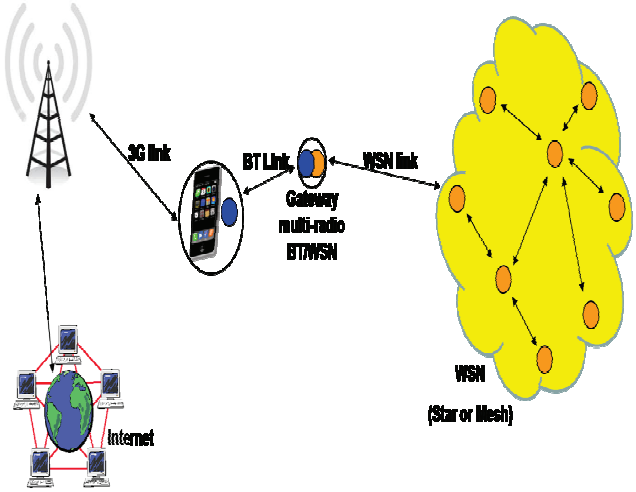

Figure 3: Architecture for indirect interoperability between a smartphone and a WSN.

V. Network Solutions for Interoperability

In this section the most important and diffused solutions will be analyzed for both direct and indirect interoperability, among a smartphone and WSNs. We will focus on the solutions based on: gateways and overlay networks also considering possible improvements [10]. In the gateway-based approach, the multi-radio device will be equipped with two radio interfaces.

According to the literature [11], different Gateway-based approaches have been proposed to interconnect generic WSN with IP-based Network. Solutions based on Application Level Gateway (ALG), sometimes, called as: *"proxy-based"*, are the simplest to perform protocol conversion and routing of data units among heterogeneous networks. Gateways/Proxies, can both operate as *relay and front-end.*

In the first case the main function is to relay data gathered by the WSN, making them available to TCP/IP network's users, where these last ones will directly be able to benefit thanks to the functionality of caching. In the second case, the Gateway is used to gather and to store preventively in a database data gathered by the WSN nodes. In this way the gateway will be considered as an interface (e.g. web interface) of a distributed system (WSN) so users will connect to it to recover the required information. The main advantage of the second approach is the simplicity of implementation and the possibility to be "transparent" for both networks.

Anyway, ALG is commonly used to develop specific functions or protocols and it is often developed *"ad hoc"* according to the specific application. Furthermore, it does not depend on the communication protocols of the WSN, but the drawback is in the absence of a "direct link" among sensor nodes and the IP users.

A possible improvement of such solution is represented by the Delay Tolerant Network (DTN)-based approach [12].

The DTN architecture is based on the new protocol level, known as "Bundle Layer" and on the store and forward message switching system [12]. This approach, recently developed for new and interesting applications [13], does not apply protocol conversion among data units. Overlay Networks refer to solutions based on: "IP overlay Sensor Networks" and "Sensor Networks overlay IP" [11]. In "IP overlay Sensor Networks", the approach radically changes in comparison with the ALG, because the functions of interoperability and protocol conversion are directly applied by the sensor nodes. In fact, IP's protocol stack is directly implemented in the WSN directly making them accessible to IP-based networks through Gateway or Edge Router with relay function.

In spite of the disadvantage that involves the implementation of the IP stack on the sensors such as an excessive cost and a higher complexity of the WSN nodes, there are a lot of works based on this solution [11-15]. IP stack implemented on the nodes will be often in "lightweight" version; some meaningful examples are the 6LoWPAN or the µIP-based approach. In "Sensor Networks overlay IP", sensor network protocol stack is implemented over IP and each IP host is considered as a virtual sensor node.

This second solution of Overlay Networks is easier and lightweight for the sensors, but the application layer at the IP side of the network needs to understand and select the packets received from all nodes of the heterogeneous network.

VI. Conclusion

In this work we have discussed possible flexible engineering solutions to guarantee the interoperability between smartphones and WSN.

The paper has discussed an application scenario where every standard for WSNs can be effectively employed together with smartphones. The architectures supporting interoperable smartphone/WSN systems, considering network topology and functionalities of the nodes, have been presented together with current network solutions for interoperability.

The solutions and the application scenarios are developed accounting for a high level of node mobility.

VII. ACKNOWLEDGEMENTS

This work was carried out as part of the TETRIS project (Servizi Innovativi Open Source su TETRA) Programma Operativo Nazionale di Ricerca e Competitività 2007-2013 funded by the Italian Ministry for Education, University and Research (MIUR).

REFERENCES

[1] X. Wu, K. N. Brown, C. J. Sreenan, "Analysis of Smartphone User Mobility Traces for Opportunistic Data Collection", Mobile Data Challenge 2012 (by Nokia) Workshop; June 18-19, 2012; Newcastle, UK.

[2] S. Yoon, Hyeongseok Oh, D. Lee, S. Oh, "Virtual Lock: A Smartphone Application for Personal Surveillance Using Camera Sensor Networks", 2011 IEEE 17th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), 28-31 Aug. 2011.

[3] G. Araniti, M. De Sanctis, S. C. Spinella, M. Monti, E. Cianca, A. Molinaro, A. Iera, M. Ruggieri, "Cooperative Terminals for Incident Area Networks", first International Conference on Wireless VITAE 2009, Aalborg (Denmark), pp. 549-553, ISBN: 978-1-4244-4067-2, 17-20 May, 2009.

[4] M. Keally, G. Zhou, G. Xing, Jianxin Wu, A. Pyles, "PBN: towards practical activity recognition using smartphone-based body sensor networks", Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems (2011), pp. 246-259, 2011.

[5] M. Pesko, M. Štular, M. Vučnik, M. Smolnikar, M. Mohorčič, "Bluetooth-based mobile gateway for wireless sensor network", The Second International Workshop on Sensing Technologies in Agriculture, Forestry and Environment, Belgrade, Serbia, 6-7 April 2011.

[6] S. Zöller, A. Reinhardt, H. Guckes, D. Schuller, R. Steinmetz, "On the Integration of Wireless Sensor Networks and Smartphones in the Logistics Domain", 10th GI/ITG KuVS Fachgespräch "Drahtlose Sensornetze", p. 49-52, September 2011.

[7] Hasbollah, "Performance analysis for 6loWPAN IEEE 802.15.4 with IPv6 network", IEEE TENCON, pag. 5, 2009.

[8]M. McInnis, IEEE P802.15.4f Active RFID System Call for Applications. http://www.ieee802.org/15/pub/TG4f.htm, 21 January 2009.

[9] M. Arsalan, A. Umair, V. K. Verma, "Dash7: Performance", IOSR Journal of Electronics and Communication Engineering (IOSRJECE) ISSN : 2278-2834 Volume 2, Issue 5 (Sep-Oct 2012), PP 08-11.

[10] J. Suhonen, M. Kohvakka, V. Kaseva, T. D. Hämäläinen, Marko Hännikäinen, "Low-Power Wireless Sensor Networks Protocols, Services and Applications", Springer Briefs in Electrical and Computer Engineering, 2012.

[11] R. Bosman, J. Lukkien, R. Verhoeven, "Gateway Architectures for Service Oriented Application-Level Gateways", IEEE Transactions on Consumer Electronics, vol. 57, no. 2, May 2011.

[12] A. Dunkels, J. Alonso, T. Voigt, H. Ritter, J. Schiller, "Connecting Wireless Sensornets with TCP/IP Networks", Second International Conference on Wired/Wireless Internet Communications (WWIC2004), pp. 143-152, 2004.

[13] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets", 2003 Conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM2003), 2003.

[14] M. Zennaro, H. Ntareme, A. Bagula, "On the Design of a Flexible Gateway for Wireless Sensor Networks", irst International Workshop on Wireless Broadband Access for Communities and Rural Developing Regions 2008, Uppsala, Sweden, 2008.

[15] J. Domingues, A. Damaso, R. Nascimento, and N. Rosa, "An Energy-AwareMiddleware for Integrating Wireless Sensor Networks and the Internet", Hindawi International Journal of Distributed Sensor Networks, Vol. 2011.

Standard	Topology	Maximum Number of Nodes	Data Rate	Coverage Range	Power Consumption	Security
IEEE802.15.4 - ZigBee	star, peer-to-peer, mesh (ZigBee)	2^16=65536 (2^64 optional)	20, 40, 250 kbps	< 1 km	40 mW	Cryptography AES 128 bit
Bluetooth - Bluetooth Smart - IEEE802.15.1	piconet, scatternet	7 nodes in one Piconet	1 Mbps ÷24 Mbps	< 100 m	200 mW	SAFER+
IEC62591 - WirelessHART	mesh	2^16=65536 (2^64 optional)	250	< 100 m	40 mW	Cryptography - AES 128 bit
ISA100.11a	mesh	2^16=65536 (2^64 optional)	250	< 100 m	40 mW	Cryptography - AES 128 bit
DASH7	star	2^16=65536 (2^32 optional)	27,7 kbps ÷ 200 kbps	< 10 km	1 mW	Cryptography - AES 128 bit
Z-WAVE	mesh	2^8 = 256	10÷40 kbps	< 300 m	80 mW	Cryptography - AES 128 bit
ANT	star, tree, mesh	2^32	1 Mbps	< 30 m	40 mW	
Wavenis	star, tree, mesh	2^32	4.8 ÷100 kbps	< 200 m	80 mW	Cryptography - AES 128 bit

TABLE 1: PERFORMANCE COMPARISON BETWEEN DASH7 AND OTHER COMMUNICATION PROTOCOLS FOR WIRELESS SENSOR NETWORKS