A Security and Privacy Survey for WSN in e-Health Applications

María de los Ángeles Cosio León,
Juan Iván Nieto Hipólito
UABC, Facultad de Ingeniería-Ensenada
Km. 103 Carretera Tijuana-Ensenada
Ensenada, B.C. MEXICO
Email: mary.cosio@gmail.com; jnieto@uabc.mx

Jesús Luna García
BARCELONA DIGITAL CENTRE TECNOLOGIC
Sancho de Avila 110-130, 08018
Barcelona, Spain
Email: jluna@bdigital.org

***Abstract*—Wireless Sensors Networks (WSN) are getting a special place in the development of e-Health application, due to its characteristics such as: not intrusive design, low energy consumption, low price and its flexibility to integrate into health care environments. However, the use of WSN in these kind of environments must consider those security and privacy mechanisms required by applicable Personal Data Protection Legislations to provide end-to-end guarantees to the patient's information. Applications and research projects are taking place to offer e-Health solutions with these features, however still there is not framework or standard to support interoperability among these or to provide a design criteria for future developments. Towards this goal, in this paper we survey a set of e-Health proposals for WSN, focusing on the mechanisms used to provide security and privacy to support real-time and multimedia data transmission in WSN.**

***Keywords*-Security; Privacy; WSN;**

I. Introduction

Wireless Sensor Networks (WSN) are a particular type of ad-hoc wireless networks that share important characteristics with related technologies (WiFi and Bluetooth). In fact many security solutions proposed for the other environments can be used also in WSN by taking into account its particular features (limited resources, in-network processing and application-specific architectures). Due to the legal requirements for protecting personal data (defined in [13] as *all data related to an individual's private, public or professional life)* and specifically a patient's information, e-Health systems that manage it (including WSN) must include specific security and privacy measures. Clearly, a WSN for e-Health could be categorized like that, since it has the capacity to provide large amounts of continuous flows of physiological data, key feature for e-Health applications that need monitoring, so in addition to technical requirements to generate, store or use patient's information, it is necessary to take into account the legal framework. The former is a difficult task because actual legislations differ among countries: for example in Europe, *the European Directives 95/46/EC* [15] and *2002/58/EC* [16] establish terms for personal data protection. In US, there are two principal acts to cover privacy, *Privacy Act of 1974 and Amendments* [19] and *National Constitution of the United States in its first amendment*. In Mexico, the protection of personal data is guaranteed by the *National Constitution (Article 16)* and two more documents, the first one giving guidelines to the protection of personal data [18] and the second mentioning a number of recommendations related to the processing of data and devices being used for this [17]. Despite its lack of harmonization, most privacy-related legislation consider the concepts of *consent and ethical restrictions* as important issues. Consent, refers to the explicit approbation about how to use a patient's personal data, ethical restrictions deal with how the subject's rights must be considered. Both concepts were studied in [9], [10]. It is important to highlight privacy-related legislation, because generally it is the final consideration in the development of e-Health applications [6], thus making difficult its integration and fulfillment. In Section 2, base WSN technologies are described. Section 3 introduces related applications and research projects that deal with WSN security and privacy proposals. Section 4 focuses on key e-Health applications using WSN and that have been designed considering security and privacy requirements. Finally, Section 5 concludes with an analysis of the surveyed proposals, again with a particular emphasis in security and privacy.

II. Underlying Technologies

The 802.15.4 [1] and ZigBee standards are key proposals for Low Rate (LR) transmissions. Their importance lies in a design considering low power consumption, reduced costs and no-intrusivity.

A. Standard 802.15.4

A 802.15.4 network faces the same problems of other wireless networks. In particular it is vulnerable to passive eavesdropping attacks and even to active tampering [14]. Most of its security related elements are implemented at higher layers. Its link layer security protocol provides four basic security services: access control, message integrity (via message authentication codes), message confidentiality (semantic security) and replay protection (based on packet counters). The application layer specifies its security requirements by setting the appropriate control parameters, but the

978-0-7695-3799-3/09 $26.00 © 2009 IEEE
DOI 10.1109/CERMA.2009.47

802.15.4 standard does not cover this layer. Frame protection can be adopted on a frame-by-frame basis and to allows modify the level of data authenticity. It may use a share key between two devices (link key) or a key shared among a group of devices, however protection is provided only against outsider devices and not against potential malicious devices in the key-sharing group.

B. ZigBee

ZigBee [2] sits on top of the IEEE 802.15.4 PHY and MAC layers. It defines some important processes to improve security and privacy: each layer improves the security level of its own data being managed; only nodes and gateways that successfully joined to the ZigBee network can receive messages; security is based on the reuse of keys by each layer; End-to-end security is enabled, so it is only possible for source and destination devices to access their shared key; the security level is maintained on all the layers and elements in the network, therefore specific requirements must be implemented as needed.

The ZigBee security architecture includes security mechanisms in a couple of layers of the protocol stack. At these layers, three kinds of cryptographic keys are used: one for the link between two nodes, another for a network and the final for management. The first one is a 128-bit key shared by whatever any two ZigBee devices. The second key is shared amongst all devices in the network. The third, is only used by the Trust Center device for key-transport and key-update. *Key establishment* occurs at Application Layer (APL). The APS sublayer's key-establishment provides a mechanism by which a ZigBee device may derive a shared secret key (Link key) with another ZigBee device by involving two entities and a starting procedure (initiator device, responder device and trust provisioning step). In a ZigBee network the master key is the security basis. This could be installed in a device via a secure or unsecure communication channel, the latter in controlled environments. This key allows devices to obtain the link key, which is fundamental for the services being provided by the application (APL) layer. A key is revoked when a device does not fulfill those security requirements assigned by for the Trust Center. There are also node update services to notice when a node joins or leaves the network. Finally there are also services to notice a change of the active network key. At the Network layer, another key is used to assure its network command frames. ZigBee includes two security modes: **Standard Mode:** In this mode, Trust Center *may* maintain a list of devices, master keys, link keys and network keys with all the devices in the network (standard network key and control policies of network admittance).
High Mode: Trust Center *shall* maintain a list of devices, master keys, link keys and network keys that it needs to control and enforce the policies of network key updates and network admittance.

III. Security and Privacy related Works

Ensuring the security and in particular the privacy of personal data being managed in WSN is an open research area, with the on-going proliferation of small devices with low-cost technologies that also consume low quantities of energy. WSN also have provided an attractive solution for many environments that require security and privacy, even though not particularly related with e-Health (i.e. surveillance, domotic, etc.). In the rest of this Section we will survey some interesting security and privacy proposals.

A. Minisec

Minisec [3] was built as secure a network layer for the Telos mote [20], which is based on Dolev-Yao attacker model, with two operating modes: unicast and broadcast, henceforth known as MiniSec-U and MiniSec-B respectively. Both schemes employ the OCB-encryption mechanism (Offset CodeBook) to provide data secrecy and authentication, specifically MiniSec-B define a mechanism for replay-attacks protection using loose time synchronization and Bloom Filter to track packet history. Minisec proposes three security mechanisms:

1-Authentication. MiniSec-U and MiniSec-B use OCB encryption to provide data authentication and confidentiality. This process applies encryption and authentication in just one step, thus achieving important energy savings. 2-Secrecy and Semantic Security. These are achieved thanks to nonces' uniqueness. The initialization vectors (IV) for the cryptosystem are sent incomplete, therefore saving energy and space on the data package. 3-Weak Freshness. In MiniSec-U, the receiver can compute a *counter value* used for each packet by verifying the validity of OCB decryption. While in MiniSec-B, this counter value is included in the packet as plaintext. In both cases, the receiver may use the counter value from two messages to enforce its ordering, thus providing *weak freshness*.

B. Tangram

Tangram [7] is a WSN algorithm proposed to improve security and privacy on images based on secret sharing and visual secret sharing, and RSA public-key cryptosystem to encrypt shares. The authors assume that: one sensor covers an specific area and each node has its own encrypted share (part of an entire image). The authors propose a new paradigm, requiring a set of private random parameters to be used in the source node for secure share generation. The proposed algorithm starts in one node, called source node, it contains an aleatory initial state independent of the image, and its first task is the generation of a value (this representing possible values for a node i, used to encrypting images). Afterwards processing these values to find the next state of the following node, they are sent the next one and destroyed in the source. Finally the information about an encrypted

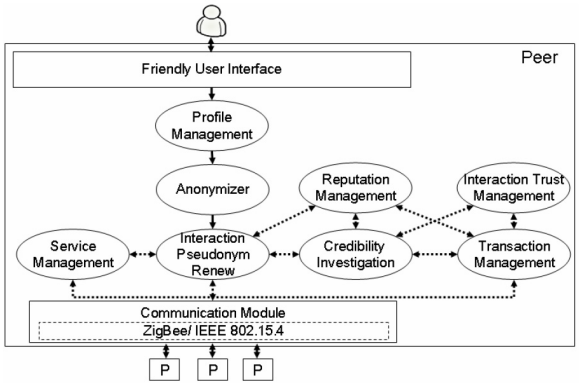

Figure 1. Collaborative iTrust platform

share is sent to base station. The entire proposal seeks to add confidentiality in a decentralized way.

C. A Privacy-Aware Identity Design for Exploring Ubiquitous Collaborative Wisdom

In [8] the authors propose a technique to use pseudonyms as a way to enforce privacy. Two types of pseudonyms are used, one that should be generated by an authorized entity and that each user should pay and, a second one (temporal) that is generated based on a root pseudonym. Executed actions (even those considered attacks) performed by temporary pseudonyms are associated with the root pseudonym. To improve privacy, the proposal uses a one-way hash function to isolate the interaction between the root pseudonym and the active pseudonym being used, thus improving the unlinkability of identities. This proposal is built over the ZigBee and 802.15.4 and the goals of using pseudonyms here when designing interactions with ambient e-services are: Exclude a unique personal pseudonym for interactions to protect users from possible tracking and profiling. Use multiple interaction pseudonyms to enhance the complexity of identity tracing. Pseudonyms design should not consider roles or relationships, because these would change the behavior of e-services.

A prototype called *Collaborative iTrust Platform* (fig. 1), integrates the entire infrastructure including the use of pseudonyms via four modules:

Profile Management: In this module each user can perform certain functions, like setting their preferences and roles they would like to play, the risk level they can tolerate and the reliability threshold for determining whether to interact with a peer nearby. Once an identity has been generated, those settings are assigned to the interaction pseudonym automatically. *Anonymizer:* Its main function is to generate temporary pseudonyms based on a given identity for various kinds of e-services. These interaction pseudonyms are only valid for a short period. *Interaction Pseudonym Renew:* this module is in-charge of a *reputation context system that*

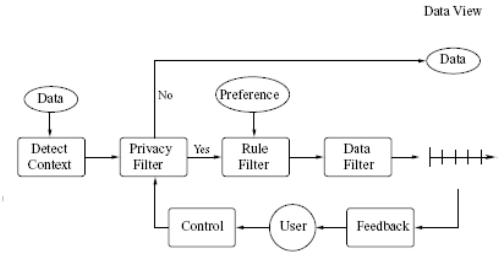

Figure 2. The basic framework for the design of a privacy sensitive smart house environment

makes all devices aware of the trust information coming from other devices. *Communication Module:* This ZigBee based module makes use of the security services are already present in the 802.15.4 security specification. ZigBee security infrastructure includes network access control, integrity of packet routing and prevention of unauthorized use of a packet transport.

D. Dynamic privacy assessment in a smart house environment using multimodal sensing

This proposal [10] is relevant to our survey due to the establishment of the privacy and personal space concepts. The authors propose a framework to implement privacy in a smart house environment by taking into account features like dynamicity and flexibility, thus providing an interface for getting feedback from users. The system is capable of modifying its performance when some of parameters being considered change The following uses-cases are considered by the authors:

Privacy in Assisted Living Smart Homes: The authors described their research to identify mechanisms to improve privacy in a smart home, concluding that: it is possible to detect a lot of activities at home with audible data, therefore a high level of privacy is possible to reach as the audio and video can be reduced to anonymous binary sensors in some cases. However, the approach also allows access to the richer datasets provided by video and audio if required by authorized entities. *Privacy-Sensitive Ubiquitous Computing Applications:* A basic framework, shownn in fig. 2, that is a synthesis of several research proposals, representing a generic approach for the implementation of privacy sensitive ubiquitous computing applications.

This scenario considers a component able to determine contextual information, generally associated with an environmental property. A second component, the privacy filter, is used to interpret the context in a binary fashion to determine if privacy measures are required or not. The combination of both, the context and privacy filters, is used for systems in which continuous privacy may not be suitable, (i.e. surveillance applications). A third component, the rule filter, is used to determine the appropriate privacy level using a rule-based approach and incorporating predefined

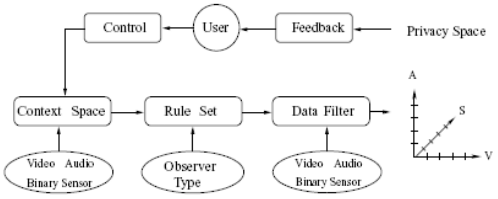

Figure 3. The extended framework for the design of a privacy sensitive smart house environment

preferences (i.e. camera turned On or Off). Finally, the feedback and control component provides information to the person being monitored, allowing them to control and fine-tune the privacy filter component.

The Second framework (fig. 3) offers a better performance. The authors introduce three concepts:

Context space: Its aim is to hide explicit information regarding the context and situations occurring within the environment to ensure the safety of the occupant, while reducing the invasion of the her/his privacy. Four outstanding factors are considered: the spatial context (where), the social context (who), the hazardous context identifying abnormal interactions with hazardous devices within the environment (how and what) and, the fourth context determining abnormal periods of inactivity (what). *Privacy space:* It is a multidimensional representation of the data access levels that are applicable to the multimodal surveillance present in the smart house. The current implementation of the privacy space for the smart house environment consists of a discrete space (audio, video and binary sensor data). *Feedback and Control:* The feedback and control mechanisms provide an interface between the occupant and the privacy system.

E. NeST: A Privacy Enhanced Software Architecture for Interactive Analysis of Data in Video-Sensor Networks

This is a test-bed and its principal objective is the access control to multimedia data with privacy facilities. NeST [5] architecture is comprised of six components: Server Core, Privacy Filtering and Security, Sensors and Interface Hardware, Knowledge base and, Activity Virtual Sensors. The authors also propose the following concepts:

The privacy buffer is a shell around the Server Core that utilizes programmable plug-in filters operating in incoming sensor data to prevent access to private information or transform data to remove personally identifiable information. Data is labeled as private or non-private by one or more *privacy filters* plugged into the privacy buffer. Privacy filters are specified with a *privacy grammar* that allows an end user to construct new privacy definitions based upon combinations of low level features and high level semantics derived from raw sensor data. NeST uses SSL for secure communication channels and client authentication with two operation modes: paranoid and apathetic. In paranoid mode it assumes that all data are private, so until a decision is taken, it will be retained on the server, during an certain period of time. On the other hand, apathetic mode passes all data to the server until a filter determines that private information is present.

Table I summarizes the main features of WSN developments surveyed in this section

IV. Security and Privacy research related with WSN in e-Health

The term e-Health is defined in [13] as the application of technological information and communications technologies through a wide range of functions that affect the health sector, from doctors to patients. The systems that handle this kind of data are very diverse and involve important challenges about secure processing, transmission and storing of personal data to cope with considerations made in applicable legislation. Due to its importance to our work, this section will review the security and privacy issues implemented in WSN e-Health applications.

A. Security issues of wireless sensor networks in healthcare applications

This paper [12] aims to introduce WSN security issues focused on healthcare requirements. The authors tackle these by describing resources on devices and corresponding security threats. The threat analysis is performed based on multiple forms of active and passive attacks. The authors describe attack that could occur in routing and packet forwarding. Take for example passive attacks which may steal and disclose information very easily via eavesdropers in a wireless communication channel. This entity is also capable of doing more harmful active attacks (i.e. by altering packets). Key management schemes serve the fundamental requirements in WSN encryption and authentication and this paper considers the following basic elements: a trusted server, a Public Key Infrastructure (PKI), a key predistribution and finally an autonomous key set-up. High level security services must be implemented for healthcare applications, where the healthcare sensor network may vary in mobility and topology, therefore requiring different sets of security mechanisms in place to suit diverse usage scenarios. On top of that, the data fusion process probably happening in intermediate sensor nodes must be also addressed along with intrusion prevention to form the secure end-to-end communication being required.
The authors' of this paper conclude that: a properly integrated security architecture is the prerequisite to ensure the successful deployment of *healthcare sensor networks*.

B. An Assisted Living Oriented Information System Based on a Residential Wireless Sensor Network

The authors propose in [11] a complete architecture, now a proof-of-concept, which integrates several devices types

Table I
A SUMMARY OF SURVEYED WSN'S SECURITY AND PRIVACY RELATED TECHNOLOGIES AND PROJECTS.

Proposal	Underlying technology	Layer implementing security/ privacy	Security Privacy features	Security Feature	Current-status	Observations
802.15.4	LR-WSN	Media-access-control	AES-128	Replay-attacks, Access-control, message-integrity, confidentiality	Implement	Protect for external attacks, weak for internal attacks
ZigBee	LR-WSN	Network-Application	AES-128	Replay-attacks, Access-control, message-integrity, confidentiality	Implement	
Minisec	Telos mote	Network	OCB-Encryption Bloom-filter loose time-synchronization	Protection versus replay attacks and Dolov-Yao attack model	Implement	Best performance obtained with Telos devices. Energy-wise design
Tangram	Free space-optical sensor network	Application	RSA public-key cryptosystem, visual secret sharing and secret sharing	Eavesdropping-attacks	Simulation	Secret sharing is an interesting proposal for WSN's privacy
e-services and pseudonyms	LR-WSN	Application	Pseudonym	Privacy	Implement	By itself is a weak mechanism to improve privacy and it needs additional features to reach it
Dynamic privacy assessment	No specific	Application	No specific	Privacy level and Privacy	Partial implementation	Privacy level could be modified by mean of sound, in other words, it is aware of environment context
NeST	PDA-802.15.4	Application	Privacy filters, privacy grammar privacy buffer and SSL	Privacy	Test-bed	Several privacy features are considered, but most over PDA-technologies

and takes into account important privacy considerations, i.e. access to a subject's sensor data requires an authorization mechanism. The current context of the patient is also taken into account because configuration rules change when an individual exhibits a behavior that is critical to his health thus enabling the authorized medical personnel to access vital data, otherwise hidden or available only for anonymous statistical purposes. The main component of the privacy framework is the propose Privacy Manager. Emergency-aware applications demand a privacy protection framework capable of responding adaptively to each patient's health conditions and privacy requirements in real time. Therefore, traditional role-based access control which makes access authorization based on users' static roles and policies is not flexible enough to manage this demand. Security features for WSN in this paper are supported by security mechanisms offered in 802.15.4 and ZigBee standards for MicaZ motes [20].

C. Multi-Stage Real Time Health Monitoring via ZigBee in Smart Homes

This is a research project that considers real time processing [4] where the authors are trying to resolve some specific gaps about ZigBee, like zero mobility and real-time acquisition for health parameters. However this is an ongoing proposal, and specific features about of security or privacy are no clear at all, although they are being considered in the project's roadmap. Security and privacy mechanisms optimized for real-time data are the basic requirement here, i.e. if an arrhythmia risk is detected, an alert will be transferred to the home server over the ZigBee network controller. If any anomaly is detected then patient's family, doctor is contacted, however his personal data should be always protected.

D. ZigBee-based alarm system for pervasive healthcare in rural areas

The authors of this paper propose an implementation for remote healthcare of elder people in rural areas [9], including security and privacy features (mostly based on the use of symmetric cryptosystems with AES-128). The envisioned network consists of mobile nodes used to detect emergency situations where a warning is sent to a central computer in the local management center (i.e. located in villages). This central computer routes the information via the Internet to the regional management center, which in turn manages alarms from several villages and provides a human operator to manage the situation. These systems involve a technology vulnerable to eavesdropping where personal parameters such as location, movement or body parameters can be captured by unauthorized entities. The authors propose a set of privacy features, but the most important issue is to obtain *informed consent* from the patients, so they are conscious of their personal data destination and use. Ethical considerations are made if potential users are unable to give their consent (i.e. in case of a life-threatening situation), in this case the patient's health is prioritized over his right to privacy. This whole project has taken into account European privacy legislation [15], [16].

Table II summarizes the main features of the e-Health and WSN proposals surveyed in this section.

V. CONCLUSIONS AND FUTURE WORKS

In this paper we have surveyed a series of WSN technologies and research projects that propose different mechanisms to cope with applicable security and privacy requirements, with tables at the end of each Section to summarize their main features and our conclusions about these particulars (tables I, II). We have found many important challenges about the security and privacy, which enforces the fact, that if a technology is safe then the people will trust on it. Otherwise its use will not be viable, even endangering the patients life. The most extensively used security and privacy mechanisms are Pseudonyms, Cryptography, and Key Sharing with the last two being implemented in 802.15.4 and ZigBee. According to the presented research and to our best knowledge, WSN security and privacy is

Table II
A SUMMARY OF SURVEYED WSN'S SECURITY AND PRIVACY RELATED TECHNOLOGIES AND PROJECTS FOR E-HEALTH.

Proposal	Underlying technology	Layer implementing security/ privacy	Security Privacy features	Security Feature	Current-status	Observations
Security issues of WSN in healthcare	LR-WSN	Not applicable	Not applicable	Not applicable	Not applicable	Overview about e-Health development requirements in a WSN
An assisted living	MicaZ	Network-Application	Security mechanisms of 802.15.4	Replay-attacks, Access-control, message-integrity, confidentiality	Partial implementation	A complete suit about privacy and security
Multi-Stage real time	MicaZ	Network-Application	*	No specific	Partial implementation	*Considerations about security and privacy are being considered, but still not specified
ZigBee based alarm	MicaZ	Application	Symmetric cryptosystems with AES-128	Privacy	Implement	Complete application making privacy and ethical considerations

organized a *secure cell*, where the out-going data needs some decoding procedures. It is necessary to propose a model that implements security and privacy End-to-End in the e-Health WSN, but at the state of the art we have not found a framework to protect continuous data flows. As future work, we plan to develop such a framework to cope with security and privacy issues related with real-time and multimedia data transmission in WSNs e-Health applications. This framework will cover the gaps identified by this survey, also considering a sensors limited features.

REFERENCES

[1] IEEE 802.15 TG4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), IEEE computer society, 2007

[2] ZigBee Task Group: ZigBee Specification, ZigBee Alliance Board of Directors. All rights reserved, 2008.

[3] Mark Luk, Ghita Mezzour, Adrian Perrig, Virgil Gligor : MiniSec: A Secure Sensor Network Communication Architecture, ACM, Cambridge, Massachusetts, USA, 2007.

[4] S. Dagtas and G. Pekhteryev and Z. Sahinoglu: Multi-Stage Real Time Health Monitoring via ZigBee in Smart Homes, IEEE Computer Society, Washington, DC, USA, 2007.

[5] Douglas A. Fidaleo and Hoang-Anh Nguyen and Mohan Trivedi: The networked sensor tapestry (NeST): a privacy enhanced software architecture for interactive analysis of data in video-sensor networks, ACM, New York, NY, USA, 2004.

[6] Compagna,, Luca and Khoury,, Paul El and Massacci,, Fabio and Thomas,, Reshma and Zannone,, Nicola:, How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach, ICAIL '07: Proceedings of the 11th international conference on Artificial intelligence and law, 2007, Stanford, California, ACM, New York, NY, USA.

[7] William Luh and Deepa Kundur and Takis Zourntos: A novel distributed privacy paradigm for visual sensor networks based on sharing dynamical systems, Hindawi Publishing Corp., New York, NY, United States, 2007.

[8] Yuan-Chu Hwang and Soe-Tsyr Yuan: A Privacy-Aware Identity Design for Exploring Ubiquitous Collaborative Wisdom, Springer-Verlag, Berlin, Heidelberg, 2007.

[9] R. Casas, A. Marco, I. Plaza, Y. Garrido and J. Falco: ZigBee-based alarm system for pervasive healthcare in rural areas, Communications, IET, IEEE, 2008.

[10] Simon Moncrieff and Svetha Venkatesh and Geoff West: Dynamic privacy assessment in a smart house environment using multimodal sensing, ACM, New York, NY, USA, 2008.

[11] Virone, G.; Wood, A.; Selavo, L.; Cao, Q.; Fang, L.; Doan, T.; He, Z.; Stoleru, R.; Lin, S.; Stankovic, J.A.: An Assisted Living Oriented Information System Based on a Residential Wireless Sensor Network Distributed Diagnosis and Home Healthcare, 2006. D2H2.

[12] Ng,, H. S. and Sim,, M. L. and Tan,, C. M.: Security issues of wireless sensor networks in healthcare applications, BT Technology Journal, 2006, Hingham, MA, USA.

[13] Jesus Luna, Marios D. Dikaiakos, Theodoros Kyprianou, Angelos Bilas, Manolis Marazakis: Data Privacy Considerations in Intensive Care Grids, Global Healthgrid: e-Science Meets Biomedical Informatics - Proceedings of HealthGrid 2008,

[14] Sasha Slijepcevic, Jennifer L. Wong, Miodrag Potkonjak: Security and Privacy Protection in Wireless Sensor Networks Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press LLC, 2005.

[15] European Commission: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.

[16] European Commission: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002.

[17] IFAI, Instituto Federal de Acceso a la Informacin, Recomendaciones sobre las polticas generales para el manejo, mantenimiento, seguridad y proteccin de datos personales, http://www.ifai.org.mx. January-2009.

[18] IFAI, Instituto Federal de Acceso a la Informacin: Lineamientos de proteccin a datos personales http://www.ifai.org.mx. January-2009.

[19] EPIC, Electronic Privacy Information Center: Privacy Act of 1974 and Amendments, http://www.epatient.org. January-2009.

[20] http://www.crossbow.com. September-2008.