Security for Pervasive Medical Sensor Networks

Oscar Garcia-Morchon, Thomas Falck, Tobias Heer, Klaus Wehrle

***Abstract*— Wireless sensor networks are going to allow for ubiquitous health monitoring, improving users' well-being, the healthcare system, and helping to quickly react on emergency situations. Meeting the strict security needs of these ubiquitous medical applications is a big challenge, since safety and privacy of medical data has to be guaranteed all the way from the sensor nodes to the back-end services, the system has to fulfill latency needs, and lots of mobility is expected.**

In this paper, we introduce a deployment model for wireless sensor networks for pervasive healthcare based on the concepts of patient area networks and medical sensor networks, and propose a complete and efficient security framework for them. Our security framework is organized into three layers, addressing the operational requirements and security needs at the patient area network, medical sensor network and back-end levels. We specify how these layers are interconnected with each other as well as the needed security mechanisms that allow for the efficient and practical deployment of secure pervasive healthcare systems based on wireless sensor networks.

***Index Terms*— Medical Information Systems, Medical Sensor Network, Patient Area Network, Security.**

I. Introduction

NOWADAYS sensor and wireless communication technologies are rapidly evolving and conquering new application areas in the healthcare domain. Wireless medical sensors ($WMSs$) are becoming smaller and more powerful, allowing for ubiquitous usage of a wide range of medical applications, such as chronic disease management. In the simplest healthcare setting, a fixed set of $WMSs$ forms the user's patient area network (PAN) allowing for health monitoring and measuring the user's vital signs. A gateway can allow the user or medical staff to access, gather, or process her medical data directly, or transmit it to a remote healthcare service. The ubiquitous use of $PANs$ enables pervasive health monitoring of users in their daily life, improving their well-being and quality of medical care, yet allowing for cost reduction in the healthcare sector [1]. Pervasive health monitoring in these diverse situations and locations is carried out by different organizations, such as surgeries, fitness centers, hospitals, or retirement homes by means of a medical sensor network (MSN) allowing authorized parties, such as medical staff, family, or sport trainers to access to the sensed health information. Thus, $PANs$ will not be isolated but will interact, coexist, and become a part of a world of professional $MSNs$, each comprising several thousands of sensors, accommodating hundreds of users's $PANs$ (see Fig. 1 and related example). The exchange of users' medical data leads to privacy and security concerns, hence basic security services are required. These concerns become especially important when a multitude of users and health institutions need to interact with each other. To the best of our knowledge, the concept of secure and safe ubiquitous medical sensor networks and patient area networks, and their underlying relationships have not been analyzed in the literature so far.

This paper addresses this open gap, and aims at describing a security framework for the pervasive use of wireless sensor networks in the healthcare domain. The contributions of this paper are manifold. First, we describe our vision for the deployment of medical sensor networks and patient area networks enabling pervasive healthcare. Second, we introduce our basic security model and the security requirements. Third, we propose a security framework enabling the deployment of secure pervasive $PANs$ coexisting with $MSNs$, comprising the

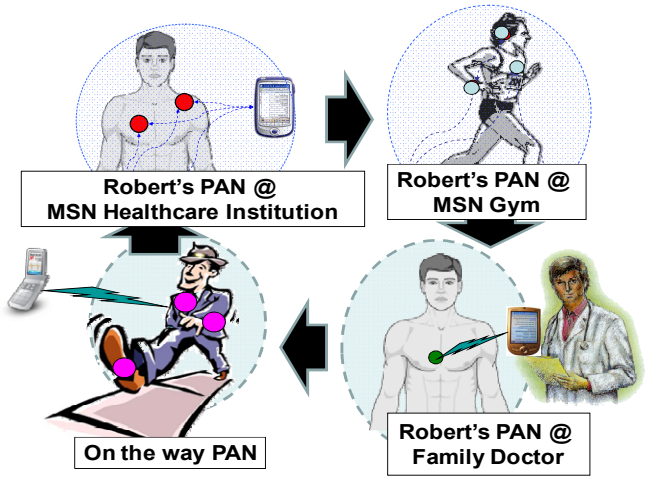

Fig. 1. Application Scenario of pervasive $PANs$ and $MSNs$: The health state of a user, Robert, is monitored in a multitude of medical sensor networks managed by a surgery, a healthcare institution, or a gym. Robert moves between those $MSNs$, and different wireless sensors such as ECG can be used in each MSN to form Robert's PAN and monitor his health state 24/7. Robert's identity should be linked to his health data independently of his location, time or medical equipment, while ensuring the privacy and security of his health data when different MSNs and back-end services interact with each other. Here, secure interaction should guarantee that medical data measured in different environments is securely transferred without endangering Robert's privacy. This paper describes our security framework and discusses the elements that enable efficient security in this context.

Manuscript received on June 5th, 2009.

O. Garcia-Morchon (oscar.garcia@philips.com) and T. Falck (thomas.falck@philips.com) are with Distributed Sensor Systems at Philips Research Europe, Netherlands.

T. Heer (tobias.heer@rwth-aachen.de) and K. Wehrle (Klaus.wehrle@rwth-aachen.de) are with Distributed Systems at RWTH Aachen University, Germany.

MSN, the PAN, and the back-end security layers Fourth, we motivate and describe the main security mechanisms needed in each of those layers. This paper pays special attention to the PAN and MSN security layers and their interactions. Finally, we provide a clear picture of the main system features, their performance, and the system operation.

The remainder of this paper is organized as follows. In Section II, we describe our vision and features of pervasive medical and patient area networks. Section III focuses on the specific security requirements of the envisioned system. Section IV overviews our security framework. Sections V-VII analyze each of the security layers of the proposed security framework. Section VIII examines the features of the system and illustrates its deployment and operation by means of an application example. Related work is discussed in Section IX. Section X concludes this paper.

II. Wireless Sensor Networks for Pervasive Healthcare: Our Vision

Health monitoring is one of the envisioned applications of $WSNs$ [1][2]. In our vision, pervasive health monitoring based on sensor nodes comprises three main functional components: the medical sensor networks ($MSNs$), the patient area networks ($PANs$), and the back-end services. An MSN is a wireless sensor network used at a specific location, and operated by a given organization such as a surgery, a fitness center, a hospital, or a retirement home. Thus, $MSNs$ are decoupled from each other as they may belong to different organizations. An MSN might comprise a large pool of wireless medical sensors ($WMSs$) used to monitor the health state of the users in that location or health institution at a given moment. Consequently, $WMSs$ from different $MSNs$ might not be interoperable on the hardware and software level because of technical incompatibilities or on the organizational level due to different security policies. A PAN is a set of $WMSs$ associated to a user for any kind of health monitoring activity. The $WMSs$ comprising the user's PAN might belong to the user (for instance, for health monitoring at home), but in most situations, they belong to a specific MSN and are only temporarily associated to that user. Therefore, the PAN membership of a user's PAN in the pervasive healthcare system depends on the user's location or healthcare institution. The medical data sensed by means of a PAN in a specific MSN can be forwarded to back-end healthcare services that ensure the system interoperability, i.e., it allows a user carrying a PAN to move across $MSNs$ operated by potentially various different organizations, while her health state is seamlessly and securely monitored.

Our model for pervasive healthcare is a combined model between traditional healthcare, in which each healthcare institution has complete control on the medical data, and a patient-centric vision [9], where the patient controls her electronic health information (EHI). In this setting, the MSN definition allows each health institution to control its own workflow and policies. The PAN supports the patient-centric vision which gives the user more control on her health information.

This pervasive use of $MSNs$ and $PANs$ presents challenging technical and operational requirements. First, the $WMSs$ are (i) resource constrained devices with just a few KB of memory, slow and short-word $CPUs$, and low-rate radios. A key requirement for health applications concerns the (ii) maximum allowed latency. For instance, real-time ECG streaming requires a latency of less than 250 msec [19], and PAN set up must be carried out within one second [18]. Especially important is the fact that the system must be (iii) scalable in multiple respects: the pervasive healthcare architecture must enable adding and integrating new $MSNs$, e.g., in a new retirement home. Besides, a stand-alone MSN can comprise thousands of $WMSs$. Finally, a PAN might comprise a variable number of devices. Another concern refers to the (iv) mobility of $WMSs$ and $PANs$ within and between $MSNs$ – a WMS can be dynamically re-associated to a different PAN within a MSN; both patients and caregivers can move within an MSN leading to frequent handshakes; besides the same patient might move between $MSNs$ and be attended in different $MSNs$ with different $WMSs$ or medical equipment. Finally, designing a healthcare system for pervasive $PANs$ must take into account real-world requirements such as the usual (v) medical workflow or operation in an emergency.

III. Security Model

A security framework for pervasive $MSNs$ and $PANs$ must ensure basic security services. *Privacy* refers to the protection of the users' identities and information from non-authorized parties. *Confidentiality* is required to protect the users' medical information in the whole system, from the sensor nodes to back-end services. System users, either patients or medical staff, as well as the exchanged medical information must be *authenticated* at any moment. Information must be protected against modification by ensuring its *integrity and freshness*. *Availability* of the measured information and medical devices must be guaranteed. *Non-repudiation* is necessary to have proof of the performed medical actions.

These security services ensure patient's safety and privacy, as required by healthcare alliances such as $HITRUST$ [2] and legal directives such as $HIPAA$ [3] in the United States and the European directive 95/46 on data protection [4]. Achieving the above security requirements requires protecting users' electronic health information (EHI) in the whole system, that is, from the PAN's $WMSs$ where the EHI is generated, to other PAN members, e.g., a clinician's PDA requesting the EHI; to the local MSN where the PAN exists at a given moment; and to the back-end healthcare services. Besides, each PAN must operate as a dynamic independent security domain within an MSN where $WMSs$ can securely join and leave at any time according to access control methods running on the PAN. The reason for this is that the $WMSs$ forming a PAN belong to the MSN security domain, but the measured medical data belongs to the user. Thus, a PAN needs to be protected and identified in a privacy-aware way so that the

PAN or sensed EHI can be neither tracked, nor linked, nor disclosed without authorization.

Besides, the specific features of $PANs$ and $MSNs$ demand specific features for the security mechanism. First, they must be energy efficient, to minimize the memory needs especially RAM, and consuming negligible amount of computational and communication resources to avoid Denial of Service attacks. Second, fast operation is needed in order to not disturb the clinical workflow, e.g. during the ward round of a doctor, and prevent attackers from launching DoS attacks. Third, scalability is a must to enable a truly ubiquitous and secure healthcare system for large numbers of $MSNs$ and mobile $PANs$. Fourth, the system must allow for the secure but unobtrusive, automatic, transparent, and verifiable association of new $WMSs$ or devices to the PAN security domain.

For our attack model, we assume that attackers have universal communication presence in the whole system. Second, we assume the existence of trusted and untrusted devices. A trusted device cannot be compromised, as we assume that it is located in a secure location or it is tamper-resistant (e.g., a smart card). An attacker might corrupt untrusted devices such as cheap sensor nodes. Third, the adversary can compromise a small ($< 20\%$) percentage of untrusted devices in each medical sensor network before being discovered. Note that this small percentage might be a high number of devices in absolute terms. Fourth, a single adversary performs node compromise; hence, all leaked information, either keying material from the MSN or the PAN or medical data, is collectively known.

IV. Overall Security Framework

We propose a security framework for the pervasive healthcare system based on $WSNs$ described in Section II. We focus on mechanisms for the privacy-aware management of the medical data and the distribution and establishment of secret keys that allow bootstrapping secure links to address the security requirements identified in Section III. We combine centralized and distributed security solutions in order to provide an adequate balance between performance and security requirements. Our security framework comprises three complementary security layers addressing the management of an MSN, a PAN, and back-end services. Each layer provides specific security algorithms as well as the physical elements and technologies needed in our framework to fulfill the specific operational requirements and ensure for seamless interaction between $PANs$, $MSNs$, and back-end services. The main features of these layers are as follows.

The MSN *security layer* allows each healthcare organization, e.g. a hospital, to manage the security in its MSN security domain. It allows any pair of devices or users in the same MSN to bootstrap a secure communication link and identify each other. For this layer, we focus on lightweight and distributed cryptographic methods for key establishment and device identification. These mechanisms are (i) lightweight to fulfill the delay requirements and save the scarce node resources, and (ii) distributed to fit the medical workflow in $MSNs$: medical staff can communicate with any PAN they encounter in a direct way, although both $PANs$ and clinicians are continuously moving. Note that this layer includes *mobile* medical sensors and devices, but also other fixed environment sensors used to measure, e.g., temperature or humidity.

The PAN *security layer* allows a user to manage the security in her own patient area network and ensures the secure disclosure of her measured medical data when interacting with $MSNs$ (e.g., clinicians in an MSN) and back-end services. The security management of this layer is centralized and it relies on a trusted device linked to and controlled by the patient.

The *back-end services security layer* ensures the secure operation of users' $PANs$ interacting with and moving between $MSNs$ controlled by different healthcare organizations. We assume a simplified centralized model for this layer based on public-key infrastructure and a single certification authority managing the healthcare system. Thus, $MSNs$ and $PANs$ just have to enroll at the certification authority to become part of the healthcare system owning some secrets such as a pair of public/private keys and a unique identifier. Note that more complex and robust models might be necessary for this layer. This paper does not cover them as our main focus is the interactions between MSN and $PANs$.

V. MSN Security Layer

The first layer of our security model for an isolated MSN is based on our previous work presented in [7]. We summarize this layer here, since the rest of the layers interact with it. The security model for a stand-alone MSN relies on a central semi-online trust center, a tamper-resistant central authority operated by the MSN administrator used for entity registration and keying material distribution. Entity refers to a wireless medical sensor or actuator carried by a user or a monitoring device used by a doctor, e.g., a PDA. Keying material refers to the cryptographic information stored in each entity and that allows for distributed key agreement, access control and identification. Semi-online trust center means that the trust center is not required for the above key agreement and access control handshakes during system operation since they are carried out in a distributed fashion.

We use lightweight security primitives based on polynomials providing full connectivity between any pair of entities belonging to the same MSN. In the basic approach [10], a single symmetric bivariate polynomial $f(x, y)$ of degree α over a finite field $GF(q)$, where q is big enough to accommodate a cryptographic key, is used to generate a polynomial share for each entity. An entity ID_z receives from the MSN trust center and stores the share $f(ID_z, y)$ generated by evaluating the original bivariate polynomial in $x = ID_z$. Whenever a pair of entities needs to agree on a common key, they exchange their identities and use their respective shares to agree on a pairwise key (see (1)) by evaluating their respective polynomial shares in the identifier of the other party. This secret key enables further security services such as confidentiality (see Section III) within the MSN by using the

AES (Advance Encryption Standard) coprocessor available in many radio chips such as the CC2430.

$$K_{ID_A,ID_B} = f(ID_A, y = ID_B) = f(ID_B, y = ID_A) \quad (1)$$

Furthermore, an entity's identifier and polynomial share can be cryptographically linked to a lightweight digital certificate (LDC), a set of information encoding the real identity and access control (AC) roles held by the MSN entity, by calculating the identifier as the hash function $hash(\cdot)$ [15] of this information [7].

$$ID_z = hash(Name, AC\ Role = Doctor) \quad (2)$$

For instance, a security handshake carried out during the operational phase of an MSN between a clinician PDA and an $ECG\ WMS$ looks as follows. First, both parties exchange their respective identifiers and use them to agree on a common key (see (1)). This pairwise key is used for entity authentication within the MSN by means of, e.g., a challenge-response handshake, session key derivation, or encryption by using the AES coprocessor present on commercial sensor node platforms [17]. Now, both PDA and $ECG\ WMS$ check the real identity or access rights of the other party by means of their $LDCs$. For instance, assuming that the $ECG\ WMS$ stores an access control policy that allows $role = doctor$ to read the ECG, the $ECG\ WMS$ can ask the PDA for its LDC verifying that (i) this role is contained in $PDA's\ LDC$, and (ii) the hash of the exchanged LDC is equal to the identifier used for key generation (see (2)).

This basic approach allows implementing a combined and very efficient security handshake for key agreement and lightweight digital certificate verification [7] fulfilling the basic operational requirements (Section III). These requirements motivate the choice of these algorithms against other solutions. In contrast to our solution, centralized security architectures can lead to high delays due to multi-hop scenarios or packet collisions [23]. Security handshakes based on public-key cryptography require several seconds on sensors leading to delays and making the system prone to DoS attacks.

VI. PAN Security Layer

The second layer is a patient-centric security layer designed to control the PAN security while interacting with the $MSNs$, for instance, controlling the sensors of the MSN associated to a user's PAN ensuring a secure communication link between them [6][16]. This section identifies and addresses the three central aspects in our design, namely (i) the physical elements, technologies, and cryptographic elements comprising the PAN security architecture (Sections VI.A and VI.B); (ii) the set up of the PAN security domain when interacting with an MSN and the cryptographic information used (Section VI.C); and (iii) the basic security services in the PAN security domain such as the management of the members of the PAN security domain, the privacy-aware identification of the PAN and generated medical data in different environments, and the provision of access control (Section VI.D).

A. PAN Security Architecture

The PAN security architecture aims at transforming a PAN into an autonomous security domain within an MSN. This security layer is based on an entity called personal security manager star (PSM^*). Next section introduces the construction of the PSM^*. The PSM^* allows the user to handle the security relationships between the $PAN's$ members so that only trusted entities, either sensors or clinician staff, are actually admitted in the PAN. A PAN does not contain MSN fixed sensors used to measure, e.g., the room temperature, but the PAN can retrieve context information from them. In contrast to the MSN security layer, the PAN security architecture is centralized because we assume one-hop (and fast) communication link around the PAN. The PSM^* is the key element in this layer since it offers the functionalities for the creation and control of the PAN security domain. This device controls the secure association of new entities and ensures high-end security services.

Observe that a PSM^* like device is needed not only in pervasive healthcare, but in any future pervasive environment where the user is surrounded or owns hundreds of devices interacting with her personal area network. The functionalities of a PSM^* are needed to handle which devices (or users) are part of the PAN, and what are their access rights on our personal area network.

TABLE I. PSM^* Security Information

Element	Target	Description
Unique Patient Identifier	HCC	Master patient identifier that identifies the patient in the healthcare system. It is used to generate PAN pseudonyms anonymizing user identity and sensed electronic health information (Section VI.D.2)
Public/Private Keys	HCC	Public-key cryptographic information used for securing the communication link between PAN and back-end healthcare systems as well as to ensure interoperability between the PAN and $MSNs$ (Section VII)
Digital Certificate	HCC	Digital certificate signed by the central healthcare certification authority containing the UPI, public key, etc.
PAN Master Key	HCC	Master symmetric key used in the PAN security domain to generate PAN keys, EHI encryption keys (Section VI.D.4) and derive privacy-aware pseudonyms (Section VI.D.2).
MSN KM	PSM	Keying material used for key agreement and LDC verification with entities within the MSN (Section V)
LDC	PSM	Information encoding the identifier and roles within the MSN and linked to the KM (Section V)
Access Control Policy	HCC	Security policy specifying the entities that are authorized to join the PAN or have access to the EHI generated in the PAN (Section VI.D.3)
Log File	HCC	Log file containing information about the PAN membership (Section VI.D.1), accesses to and actions carried out in the PAN (Section VI.D.5)
PAN EHI Record	PSM	Secure patient-centric health record containing the encrypted EHI generated in the PAN (Sections VI.D.4 and VI.D.5)

B. Patient Security Manager*

The PSM^* of each user combines two different physical devices to organize the security relationships between the PAN members within and between different $MSNs$. These two devices are a healthcare card (HCC) that belongs to the patient, and a PSM that belongs to the MSN. The HCC is tamper resistant to protect secret information (See Table I). The PSM^* is activated by plugging the patient's HCC into the PSM. We differentiate between PSM^*, PSM and HCC patient to keep in mind the workflow in $MSNs$ and pervasive healthcare systems. While the healthcare card is a token tied to and owned by the patient, the PSM is controlled by the MSN and might be different in each MSN according to specific MSN interfaces. Note that a PSM might take a multitude of physical forms depending on the location or specific use – it might be a bracelet, a mobile phone or a tag. The patient's healthcare card acts as link for the patient's identity between different MSN security domains, e.g., hospitals or fitness centers. The patient's healthcare card plugged into an MSN PSM form the patient's PSM^* for that MSN. The PSM^* manages the PAN security relationships between the entities associated to the PAN in that specific MSN and the back-end healthcare services. Healthcare smart cards are already in used in countries like Germany [18] for identification and payment. We specify additional functionality for our HCC focusing on the security management of pervasive $PANs$. On the other hand, the $PSMs$ are devices whose scope is limited to the MSN in which the $PSMs$ operate. Each PSM stores the MSN keying material that ensures efficient intra-MSN security as explained in Section V, and thus, it serves as secure interface between the patient's HCC, which actually contains the patient's information, and the MSN entities. Table I specifies the stored information on the PSM^*.

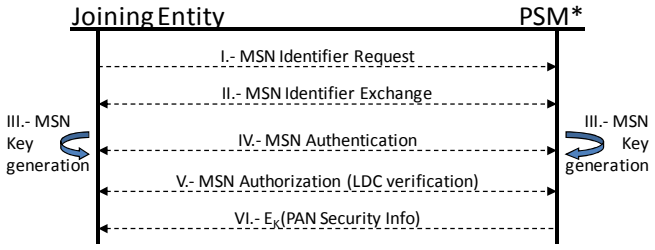

Fig. 2. Secure Entiy Association Phase

C. Setting up the PAN Security Domain

Setting up the PAN security domain comprises two basic steps, PSM^* configuration and secure entity association.

The PSM^* is configured when a patient joins the MSN by inserting her HCC into a PSM. At this moment, a security handshake (based on public key cryptography, see Section VII) is carried out for mutual identification and authentication of patient and MSN. Next, the HCC communicates with the health certification authority to request specific configuration information for that MSN such as access control policies. Finally, the MSN trust center distributes a set of MSN keying material to the PSM^*. This keying material is linked to the patient's lightweight digital certificate and contains the basic patient identification information. This information is used to set up a secure communication link between PSM^* and MSN entities within the MSN as described in Section V. Once the PSM^* is configured, it is used for secure PAN association based on body-coupled communication (BCC), i.e., determines which sensor nodes belonging to the MSN can form a part of the PAN. This protocol extends our previous work in [6] where we focused on the unsecure association of an isolated PAN. BCC is a competitive communication technology for body area networks due to its low energy requirements, and low inference level with respect to traditional wireless communication [5][6]. BCC also has inherent advantages for security since communication is restricted to the human body preventing attackers from injecting forged messages or eavesdropping on the communication [5][12]. Therefore, our security framework requires the PSM^* and $WMSs$ to be outfitted with a BCC interface. Fig. 2 depicts the procedure followed for secure BSN association between the patient's PSM^* and an MSN entity trying to join her PAN. This general protocol is carried out via the BCC channel, and thus, it is restricted to those devices directly attached to the patient's body. Steps I-V refer to the intra-MSN security handshake explained in Section V.

If the entity is authorized to join the PAN, the PSM^* sends (step VI) the PAN security information to the entity. This information includes the current (i) PAN pseudonym, (ii) PAN key K_{PAN-i}, (iii) key to secure the sensed EHI $K_{(EHI|i-r)}$ with access control level r, and (iv) LED blinking sequence. This communication link is secured by means of the pairwise key (step III) generated from the MSN polynomial keying material (Section V). The PAN security information is updated regularly differentiating sets of information from different sessions. A session S_i is a period of time, e.g., one hour, during which a PAN employs the same set of PAN security information. The PAN key is the network key of the PAN's security domain. It is used for secure broadcast of PAN configuration information within the PAN. As in [16], the $LEDs$ of the $WMSs$ associated to a PAN synchronously blink following a LED blinking sequence in order to allow clinicians to visually check the correct PAN association of all the $WMSs$ in a simple way. The functions and details of the PAN pseudonyms and EHI protection mechanism are explained in Sections VI.D.3 and VI.D.4 respectively.

D. The PAN Security Domain

The PAN security domain must ensure that the user's medical information is not misused or disclosed in a non-authorized way. To this end, this section identifies and discusses mechanism for: (i) entity management in the security domain (Section VI.D.1), (i) privacy-aware identification of a PAN in different $MSNs$ at different moments (Section VI.D.2), (iii) entity access control enforcing that only authorized parties are allowed to join the PAN (Section VI.D.3), and (iv) EHI access control ensuring that the measured EHI in the PAN security domain cannot be decrypted without proving the necessary access rights (Section

VI.D.4). Basic security services such as confidentiality (Section III) are assumed to be provided by means of standard symmetric efficient algorithms.

1) PAN Membership Management

The capability of adding and removing entities from a PAN security domain in a dynamic and secure way ensures that only authorized entities interact with the PAN. The PSM^* manages the PAN members, namely wireless medical sensors and clinicians. $WMSs$ sense the user's vital signs, and the clinicians monitor the sensed patient's vital signs by means of a clinician's PDA.

The PSM^* discerns during the secure entity association phase (steps IV - V) whether an entity is a WMS or clinician as this information is encoded in the $LDCs$. The PSM^* handles these entities in a different way. On the one hand, on-body $WMSs$ (e.g., ECG) might be attached to or removed from the patient body by clinical staff or just accidentally fall off leading to false measurements. Thus, the PSM^* periodically sends requests to each WMS registered to the PAN via BCC. If the PSM^* does not receive a reply from one of them, the PSM^* knows that the on-body device is not in direct physical contact anymore, and thus, the device is removed from the SD. To this end, the PSM^* sends a new PAN pseudonym, PAN key, and LED blinking sequence to each PAN member. Communication links between the PSM^* and each node are secured by the pairwise key generated with the MSN keying material (Section V). Note that this step prevents attackers from using the old keying material stored on the leaving WMS to eavesdrop on the PAN communication links. The strategy for other out-of-body $WMSs$, e.g. X-ray machines is slightly different. The joining procedure takes place as above, but it expires after a given period of time. On the other hand, clinicians belonging to a PAN are only removed due to changes in the access control policies, e.g., due to a context change like change of ward. In this case, the PSM^* updates the PAN identifier, PAN key and LED blinking sequence following the same procedure describe above.

2) PAN Privacy-Aware Identification

Using a global unique PAN identifier (UPI) for the whole system is needed to link the medical data measurements in different locations ensuring interoperability, but can lead to privacy concerns. Thus, identity protection is provided by using a hierarchy of pseudonyms to name a single PAN in a different way in each MSN instead of the UPI directly. These pseudonyms derive from the global UPI but cannot be linked without authorization of the patient or the central healthcare CA preventing an unauthorized user from tracking the patient or linking the real patient identity to her medical data generated in the PAN. We distinguish between *master and session PAN pseudonyms* in each MSN. The first one $ID_{PAN|MSN}$ identifies the PAN in the MSN. This is the only user identifier known to an MSN, i.e., the MSN does not know the UPI. $ID_{PAN|MSN}$ is authenticated during the set up of the PAN security domain (Sections VI.C and VII) and generated by applying a hash function to three parameters: the UPI, the MSN identifier ID_{MSN}, and the PAN master symmetric key $K_{Master-UPI}$:

$$ID_{PAN|MSN} = h(UPI||ID_{MSN}||K_{Master-UPI}) \quad (3)$$

The second pseudonym is derived from the $ID_{(PAN|MSN)}$ to anonymize the PAN identity within the MSN for the current session S_i.

$$ID_{PAN|MSN-i} = h(ID_{PAN|MSN}||h(K_{Master-UPI}||ID_{MSN})||S_i) \quad (4)$$

Each pseudonym identifies the PAN at a specific location and time span. An attacker cannot link pseudonyms to the user's UPI since he lacks the required secret $K_{Master-UPI}$. On the contrary, the central health CA and the user have access to this secret that they can prove, if needed, that any pair of pseudonyms belong together. The secret $h(K_{Master-UPI}||ID_{MSN})$ is known to the MSN trust center so that the MSN can link the different pseudonyms of a PAN within its MSN security domain.

3) Entity Access Control

The PSM^* is used to ensure PAN access control, i.e., to decide whether a PAN member is allowed to do something or not. This is done in a distributed manner from the MSN point of view but in a centralized fashion from the PAN view point.

We implement a context-aware role-based access control system. Role-based access control is enabled by encoding the access control roles of an entity, e.g., a doctor, in the lightweight digital certificate issued by the MSN trust center (Section V). The roles are assigned during the entity enrollment phase at the MSN. When an entity tries to join a PAN, the PSM^* verifies the roles held by the entity following the general protocol in Section VI.C. Context-aware access control policies are stored on the PSM^* during patient admission in the MSN and can be dynamically controlled by the user's PAN. The context-aware access control policy dynamically grants access depending on the context. Considered context variables include health state, location, time as well as external variables such as room temperature. Authentication of the context sources (e.g., fixed MSN sensors) is required to ensure the system security. This approach enables access to the PAN to any clinician, e.g., when an emergency is detected [22]. Note that this paper does not include all the details due to place constrains.

Fig. 3 depicts the overall entity access control procedure. On the left side, we see the configuration phase in which the different MSN entities receive a set of KM linked to an LDC as described in Section V. Note that this configuration phase can take place at different times, e.g., the PSM^* is configured with KM during patient admission in the MSN (Section VI.C). On the right side, we observe a PAN comprising the PSM^* and a WMS. When a clinician PDA requests the readings from a $PAN's$ WMS (step 1), the PSM^* firstly verifies that the PDA holds the correct roles for the current context. If this step is successful, the PDA joins the PAN security domain and the PSM^* sends a request to the WMS (step 2) to start broadcasting the required information (step 3). Observe that this procedure is centralized from the PAN view point but distributed for the MSN since the MSN trust center is not

involved in this security handshake. This minimizes the delays during normal system operation [7].

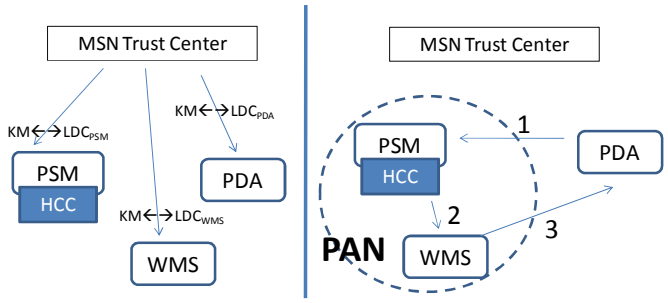

Fig. 3. Enity Access Control Procedure

4) EHI Management and Access Control

After receiving a graphic or a set of graphics, the tool will check the files against a set of rules.

We use a PSM^* centric approach for the secure storage and processing of the electronic health information (EHI) sensed in the PAN security domain. We derive two secrets from the master symmetric key K_{Master}. First, we generate the PAN key K_{PAN-i} for the current session S_i as $K_{PAN-i} = h(K_{Master-UPI}|0|S_i)$. The PAN key is used to create a PAN security domain wherein the basic transmissions, e.g., for PAN configuration, are encrypted and authenticated.

Second, we adapt the lightweight approach described of Sorniotti et al. [10] to enable controlled access to the EHI depending on the corresponding access control restrictions. This approach is based on an EHI access control hash chain for the current session S_i. We generate the anchor of the hash chain as $h(K_{Master-UPI}|1|S_i)$, and the r^{th} element of the chain $K_{(EHI-i|r)}$ is calculated by applying r times a hash function on the anchor. This hash chain has t links. The PSM^* categorizes the medical data in a total of t access control levels. The smaller the access control level AC_L, the higher the restrictions to have access to the information. Thus, each WMS that joins the PAN is assigned to an AC_L between 1 and t, depending on the type of EHI collected and current context, and receives the corresponding encryption key $K_{(EHI-i|AC_L)}$ from the EHI access control hash chain. The WMS encrypts the sensed PAN vital signs with this key and sends this information to the PSM^* that is in charge of securely storing this information. This simple approach enables two key functionalities, namely access control broadcast and secure EHI storage.

Access control broadcast allows several clinicians with different access rights to access the user's EHI in real time without need of unicasting the information to only those clinicians with sufficient access rights. If a clinician requires access to the EHI, the PSM^* checks his access rights for the current context and assigns him an AC_L for the current session S_i receiving the current EHI key $K_{(EHI-i|AC_L)}$. Now, the clinician can access all the encrypted broadcasted EHI in the PAN encrypted with access control level AC'_L with $AC_L \geq AC'_L \geq t$. Note that this is possible as the keys are generated by means of a hash function, i.e., given an intermediate hash chain element, it is only possible to generate the following chain elements. Note again that we differentiate between entity (Section VI.D.3) and EHI (Section VI.D.4) access control.

The *encrypted medical data* is stored on the PSM for fast access to the patient health record together with some unencrypted identification information including the PAN pseudonym, the session pseudonym; and the access control level. A keyed-hash message authentication code $HMAC_K(m)$ [15] calculated as the keyed hash of the fingerprint of the stored information, (see (5)) is attached to the EHI allowing for integrity.

$$HMAC_{h(K_{Master-UPI}||ID_{MSN})}(h(EHI|ID-i-AC_L)) \quad (5)$$

This information allows the user or back-end services to verify that the encrypted medical data has not been modified, since it is protected by the $HMAC$ and the secret $h(K_{Master-UPI}||ID_{MSN})$.

For further protection of the EHI generated in the PAN security domain, $WMSs$ allow for automatic memory erasing. This is triggered on a WMS if it detects that it has not been in close physical contact with the patient's body for a time longer than $T_{Threshold}$. Observe that this is possible since body coupled communication is used between $WMSs$ and the PSM^*. The automatic memory eraser rewrites all the memory data pages used to buffer and store sensed EHI preventing an attacker from recovering private patient information.

5) Data Logging

All the actions carried out within the PAN are recorded on the user's HCC. This guarantees auditing of medical actions since the user's HCC can keep a record of all the $WMSs$ and clinicians who tried to have, or had access to the user's PAN. The technical properties (tamper resistant nature and user PIN) of smart cards prevent unauthorized access to this information. Finally, the EHI is securely stored on the PSM for fast access.

VII. Back-End Security Layer

The last layer of our system relies on public-key cryptography (PKC) aiming at the fully secure interoperability of $MSNs$ and $PANs$. This paper assumes a single and centralized healthcare certification authority for simplicity, however more complex trust models are expected. Each user of the healthcare system owns a pair of public/private keys linked to the user's unique patient identifier by means of a digital certificate signed with the CA's private key. This information is stored on the user's HCC. $MSNs$' trust centers must also register with the healthcare CA and receive a pair of public/private keys signed with the CA's private key. Our security framework limits the use of PKC to two situations. First, the set up of a secure communication link between PAN and back-end services requires a public-key based handshake. This occurs in very specific situations. For instance, when a user joins an MSN and the user's HCC needs to securely communicate with back-end services for storage of the sensed medical data or to retrieve access control policies for the MSN. Second, PKC is also used for mutual authentication of a user and an MSN during the set up phase of the PAN SD

(Section VI.C). The centralized health CA keeps a backup of the most relevant PAN secrets stored on the HCC (e.g. to address the lost of a HCC) of each user including the unique $PAN's$ identifier and the $PAN's$ master secret. This can be done efficiently by deriving the $PAN's$ master secrets $K_{Master-UPI}$ from a global master secret K by means of a one-way hash function as $K_{Master-UPI} = h(K|UPI)$. The UPI and master symmetric secret are used to generate all the pseudonyms and symmetric keys used in the PAN. Therefore, the health CA can determine whether EHI sensed in different $MSNs$ belong to the same user or not. This is needed for interoperability reasons between $MSNs$.

VIII. System Evaluation

This section analyses the security, performance, and operation of the proposed security framework.

A. Security Properties

This section discusses the security properties of our system revising the high level security goals of Section III. We do it at high level as the system includes many different features. A more detailed analysis is not possible due to place limitations.

Privacy and access control are key problems. We use pseudonyms to decouple the patient's identity in different locations. Only authorized clinical personal can join a PAN and access its data as each clinician receives a different access right level depending on the roles encoded in her certificate (entity access control). A clinician can decrypt more or less information depending on this access right level (medical data access control). Both pseudonyms and access control rights are regularly updated, ensuring that only authorized personal can link measured EHI at different locations or times.

Confidentiality is ensured in different ways. For the medical data, the system encrypts the sensed data on the nodes. The information is only disclosed to authorized personal. The security information exchanged between nodes in an MSN is protected by means of the pairwise keys generated with the MSN lightweight solutions. Here, we assume the use of the AES coprocessor present on commercial radio-chips such as the $IEEE$ 802.15.4 compliant $CC2430$. Besides, the exchange of security information occurs over a body-coupled communication (BCC) channel at the PAN. Experiments prove that BCC propagation out of the body is around 20 or 40 dB weaker than conventional wireless technology [12]. Hence, it prevents attackers from eavesdropping on the security link and limits access to the information to those nodes in direct physical contact. Finally, BCC also allows for automatic memory erasing, ensuring the data is not disclosed if a node is removed from the PAN.

Entity authentication is ensured at different levels. The back-end security layer provides users with a master identity linked to master secrets and a public-key. This information can be used to identify and authenticate the user in the whole system. At the MSN level, we rely on the keying material issued by the MSN trust center. This keying material is linked to unique identifiers in a given MSN, and thus, allows for implicit entity authentication.

Message authentication, integrity and freshness are not directly addressed in this paper. They can be enabled by standard symmetric techniques on commercial radio chips.

B. System Performance and Availability

This paper aims at describing the interaction between $PANs$ and $MSNs$ and the needed elements for their secure deployment. This section analyzes the performance of the main algorithms, their impact on the system, and our design decisions. As proof of concept, we have implemented and tested the lightweight algorithms of the MSN and PAN security layers on the Philips AquisGrain sensor node.

We limit the use of public key cryptography (PKC) since the execution of PKC operations requires several seconds [13] on a typical resource-constrained sensor node platform [17] inducing high delays and making the system prone to denial of service attacks [7]. Thus, its use is restricted to those procedures in which the performance is not a limitation or its use inevitable, e.g., the bootstrapping phase of a PAN, and communication with the back-end layer. Here, we assume the use of standard public-key cryptography, symmetric encryption, and hash algorithms.

For the MSN layer, we opt for the polynomial-based security handshake (Section V) that can be executed in a few milliseconds [7][21] (Table II) as verified during our tests. Note that system availability is one of security requirements in Section III, and the reason to use lightweight cryptographic primitives for the resource-constrained $WMSs$, reducing the energy use and delays, and preventing attacks. The design of the MSN layer is performed assuming that an attacker cannot compromise more than a given percentage (e.g., 20%.) of the nodes in the network. In this system, we consider the use of at least 80-bit long keys. Table II includes additional configuration and performance parameters for different network sizes. The system performance is measured by the number of required 16-bit modular multiplications (CPU word size on a sensor node) for key generation, the maximum security provided by an LDC, and the overall expected time for a combined key agreement and LDC verification handshake. Note that this paper does not include the details of those algorithm optimizations due to space reasons. They will be published somewhere else [7]. The relative resiliency refers to the percentage of nodes in a network of size N that are to be compromised to break the system. Thus, our MSN design seeks a trade-off between availability, offered security level, system configuration and performance in this layer.

TABLE II Configuration and Performance Parameters

N	Relative Resiliency	Memory	Number of Multiplicat.	LDC Security	Time
1000	24%	1997 B.	160	110 bit	13 ms.
2000	24%	4028 B.	220	105 bit	16 ms.
5000	19%	8089 B.	360	99 bit	23 ms.

The PAN security layer is also very efficient. We only use mechanisms based on symmetric cryptography several orders of magnitude faster than PKC [15]. Body-coupled communication requires much less energy than typical

wireless communications, and thus, this minimizes the energy consumption of the system. The system uses pseudonyms and $HMACs$ generated by means of a hash function. Our practical measurements showed that the calculation of a 128-bit hash operation (AES −based Matyas-Meyer-Oseas hash function [22]) requires 0.8 ms. In this part of our implementation, we reserve 500 bytes for our context-aware access control policies requiring less than one millisecond for the evaluation of a simple logic. Finally, the EHI-access control approach used has been proved to be feasible for sensor nodes [10].

C. Deployment and Workflow: Use Case

Robert, our user in Fig. 1, has joined a new pervasive healthcare system offering strong security services as he wants to protect and control the disclosure of his own EHI. At home and on the way, his cell phone runs a generic health application that allows home monitoring of Robert's vital signs measured by means of a set of $WMSs$. Robert can plug his HCC into his phone creating a secure link with back-end services and identifying himself. Sometimes Robert has to go to the hospital for a regular medical examination. When Robert arrives at the hospital's admission desk, he uses his HCC for identification and billing. Afterwards, the HCC is inserted into a hospital PSM and a mutual authentication handshake is carried out based on public key cryptography. The PSM^* is configured with the corresponding keying material, lightweight digital certificate, and access control policy for the hospital MSN at this step after secure access with the central healthcare CA. Later, a nurse simply attaches a set of $WMSs$ to Robert's body. Each $WMSs$ automatically communicates with Robert's PSM^* carrying out a key agreement, authentication and authentication handshake over BCC. Each WMS that successfully finishes this step becomes a member of Robert's PAN receiving his PAN network key and the current Robert's pseudonym. These nodes form an independent security domain protecting Robert's privacy sphere. The identities of nurse and $WMSs$ are stored on the Robert's HCC log file. As a doctor wants to monitor Robert's vital signs, he briefly touches him, establishing a BCC channel between PSM^* and her PDA and completing an authentication and authorization handshake. If the clinician holds enough rights, the PSM^* admits her in Robert's PAN so that she receives Robert's security information including PAN key and EHI key that allows her to access Robert's EHI.

IX. Related Work

The main contribution of this paper is the design of a security architecture considering the concepts of MSN, PAN, and their inherent relationships. This problem has not been addressed before for the best of our knowledge. For related work on BCC, polynomial schemes, and access control we refer to the references included in previous sections. The PAN set up problem is discussed in [16],[6],[24], but it is not performed in a secure manner. In [25] the authors present an approach that allows devices on the body measuring the same physiological values to generate a cryptographic secret. This approach allows securing a cluster (PAN) topology formation. However, this scheme presents three main drawbacks. First, it is still an open issue the secure connection of on-body with off-body devices since the latter cannot measure physiological parameters of the user. Second, the assumption that all sensors can measure a common vital sign does not hold in practice. Third, related approaches for key generation based on ECG (e.g., [26],[27]) require a very precise time synchronization between sensors and substantial processing power on the medical sensors. In [28] the authors describe a trust model based on public-key cryptography with some similarities to our PSM^*. However, this system does not address (i) the specific interactions between $MSNs$ and $PANs$ and (ii) the provision of services such as privacy-aware identification. The provision of an end-to-end secure link [36] is not enough as arbitrary $WMSs$ must be associated to the user's identity. The requirements of medical sensor networks have been studied in a number of papers. In [33], the main security issues are analyzed and key management is pointed out as the central problem. J. Misic and V. B. Misic have worked on the area of security and medical applications contributing many publications such as [32]. Researchers at Harvard University [31] and Imperial College [34] have pointed out the use of public-key cryptography to set up secure communication links between body sensor nodes (our MSN security layer). However the performance of public-key primitives is prohibitive for many real-world settings involving mobility. Besides, those schemes do not address other important features such as the interactions of $PANs$ with different $MSNs$. Finally, related work to identification, privacy protection, or access control have been studied in, e.g., [29] or [35] being applied to HealthGrid and not to sensor networks.

X. Conclusions

Pervasive healthcare solutions based on sensor networks are starting to be deployed. This paper proposes a flexible and extensible security framework that addresses both the healthcare institution centric approaches predominant today and the future patient-centric vision for healthcare systems by introducing the MSN and PAN security layers. Both layers are interconnected by the back-end security layer enabling a unique, interoperable and secure pervasive healthcare system.

To address the specific legal [2][3][4] and operational [7][19] needs of the system, we combine strong security primitives such as public-key cryptography with lightweight cryptographic primitives at the MSN and PAN layers providing a trade-off between security, availability, and efficiency. We further introduce key security mechanisms and protocols running at the PAN security layer, such as the methods to configure a PAN when a user joins an MSN, distributed access control approaches, and privacy-aware PAN identification in the whole system. Our preliminary performance and operation analysis shows that our security architecture can operate in a very efficient way without modifying the expected medical workflow.

Simplicity is keep in mind for easy, autonomous, and

transparent management of the whole system in professional environments where users without technical background must be able to intuitively handle the (security) appliances given to them. Our overall design accomplishes this by moving all the set up procedures for PAN security to the moment when a user joins an MSN. Here, the application of a tamper resistant healthcare card for PAN identification and security administration simplifies the PAN management and ensures PAN interoperability in the whole system of $MSNs$. Afterwards, the PSM^* can supervise the PAN and its security relationships within the MSN in an autonomous fashion. The use of body-coupled communication makes handling with a PAN extremely intuitive, as sensors only need to be attached to the patient's body and the PSM^* automatically and securely configures them as members of the PAN security domain.

This paper provides, therefore, a comprehensive view of the whole security framework, including security algorithms, technologies, and procedures, specially designed to allow for the secure deployment of wireless sensor networks for pervasive healthcare applications.

REFERENCES

[1] U. Varshney, "Pervasive Healthcare" Computer, vol. 36, no. 12, pp. 138-140, Dec., 2003.

[2] The Health Information Trust Alliance (HITRUST) (online available at www.hitrustalliance.org).

[3] The US Congress, Health Insurance Portability and Accountability Act. Washington D.C., 1996. (online available at http://www.hhs.gov/ocr/hipaa/).

[4] The European Parliament and the Council of the European Union, Directive 95/46/EC (online available at http://www.cdt.org/privacy/eudirective/EU_Directive_.html)

[5] A. T. Barth et al., "Body-Coupled Communication for Body Sensor Networks," in proc. Of the ICST 3rd International Conference on Body Area Networks, 2008.

[6] T. Falck, H. Baldus, J. Espina, and K. Klabunde, "Plug'n Play Simplicity for Wireless Medical Body Sensors," in proc. of Pervasive Health Conference and Workshops, 2006 , vol., no., pp.1-5, 2006

[7] O. Garcia-Morchon and H. Baldus, "Efficient Distributed Security for Wireless Medical Sensor Networks," in proc. Of ISSNIP 2008.

[8] O. Garcia-Morchon, L. Tolhuizen, T. Heer, and K. Wehrle, "Lightweight Key Agreement and Digital Certificates for Wireless Sensor Networks," Submitted to ACM CCS 2009.

[9] "Patient-centric: the 21st century prescription for healthcare" Healthcare and life science, July 2006.

[10] A. Sorniotti, R. Molva, and L. Gomez, "Efficient access control for wireless sensor data," in proc. of PIMRC 2008, IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 15-18 September, 2008, Cannes, France.

[11] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," in proc. of Conf. Advances in Cryptology (Crypto'92), E.F. Brickell, ed., pp. 471-486, 1992.

[12] J. H. Hwang, and S. W. Kang,"Radiation characteristics of HBC and its comparison with wireless communication," IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) May 2008. Available online at https://mentor.ieee.org/802.15/documents?n=19

[13] A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," in proc. of the 7th International Conference on Information Processing in Sensor Networks (IPSN 2008), SPOTS Track, pages 245-256, 2008.

[14] Smart Card Alliance – White Paper, "HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements" September 2003 (www.smartcardalliance.org/pages/publications-hipaa-report)

[15] A. J. Menezes, P. C. Van Oorschot, and S. C. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, 1996, (online available at http://www.cacr.math.uwaterloo.ca/hac/).

[16] J. Andersen and J.E. Bardram, "BLIG: A New Approach for Sensor Identification, Grouping and Authorization in Body Sensor Networks," in proc. of 4th Int. Workshop on Wearable and Implantable Body Sensor Networks, (BSN 2007), March 26-28, 2007.

[17] Datasheet of the MICAz mote MPR2400CA – Document part number: 6020-0060-04 Rev.

[18] ZigBee Allicance, "Personal, Home, and Hospital Care: Technical Requirements Document" Release 075111r02, September 2007.

[19] C. Cordeiro and M. Patel, "Body Area Network Stardardization: Present and Future Directions," in proc. Of 2nd International Conference on Body Area Networks (BodyNets 2007), June 2007.

[20] O. Garcia-Morchon, H. Baldus, and D.S. Sanchez, "Resource-Efficient Security for Medical Body Sensor Networks," in proc. of 3rd international Workshop on Wearable and Implantable Body Sensor Networks (BSN 2006) April 03 - 05, 2006.

[21] D. Sanchez and H. Baldus, "A Deterministic Pairwise Key Pre-Distribution Scheme for Mobile Sensor Networks," in proc. of SecureComm 2005.

[22] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring," Technical Report CS-2006-11, University of Virginia, 2006.

[23] G. Perbellini, P. Garino, O. Garcia-Morchon, H. Baldus, A. Willig. "ANGEL Deliverable D2.3: Complete co-simulation framework and refined models of the components of the Angel platform" ANGEL FP6 EU funded project (www.angel-ist.eu)

[24] H. Baldus, K. Klabunde, G. Müsch, "Reliable set-up of medical body-sensor networks," in proc. of 1st European workshop on wireless sensor networks (EWSN 2004), Berlin, In LNCS. Springer, Berlin Heidelberg New York, pp 353-363.

[25] K. Venkatasubramanian and S. Gupta, "Security For Pervasive Health Monitoring Sensor Applications," in Proc. of 4th International Conference on Intelligent Sensing and Information Processing (ICISIP'06), Bangalore, India, December 2006, pp 197-202

[26] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "EKG-based Key Agreement in Body Sensor Networks," in proc. of 2nd Mission Critical Networks Workshop, IEEE Infocom Workshops, Phoenix, April 2008.

[27] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," IEEE Communications Magazine, vol. 44, no. 4, pp. 73-81, 2006.

[28] C. Gehrmann, T. Kuhn, K. Nyberg, and P. Windirsch. "Trust model, communication and configuration security for Personal Area Networks," in proc. of IST Mobile Summit 2002

[29] Zhang, N. et al. "A Linkable Identity Privacy Algorithm for HealthGrid," in: Solomonides, T. and McClatchey, R., (eds.) From Grid to Healthgrid. Proceedings of Healthgrid. IOS Press, pp. 234-245.

[30] CodeBlue: Wireless Sensors for Medical Care – Harvard University. Available online at http://fiji.eecs.harvard.edu/CodeBlue

[31] V. Shnayder, B. Chen, K. Lorincz, T. Fulford-Jones, and M. Welsh, "Sensor Networks for Medical Care", April, 2005 Available online at http://fiji.eecs.harvard.edu/biblio/keyword/2

[32] J. Misic and V. B. Misic, "Wireless Sensor Networks for Clinical Information Systems: A Security Perspective," in proc. of 26th International Conference on Distributed Computing Systems, 2006.

[33] H. S. Ng, M. L. Sim, and C. M. Tan, "Security Issues of Wireless Sensor Networks in Healthcare Applications," British Telecom Technology Journal 24 (2): 138-144, APR 2006.

[34] S.L. Keoh, E. Lupu, and M. Sloman, "Securing Body Sensor Networks: Sensor Association and Key Management," in the Proc of PerCom 2009, Galveston, Texas, March 9 - 13, 2009.

[35] W. Jih, S. Cheng, J. Hsu, T. Tsai. "Context-aware Access Control in Pervasive Healthcare" In Proc. Of EEE'05 Workshop: Mobility, Agents, and Mobile Services (MAM 2005).

[36] V. Gupta et al, "Sizzle: A Standards-Based End-to-End Security Architecture for the Embedded Internet" in proc. of PerCom, 2005.