SECURE WEARABLE AND IMPLANTABLE BODY SENSOR NETWORKS IN HAZARDOUS ENVIRONMENTS

Mohamed Hamdi, Noureddine Boudriga
Communications Networks and Security Research Lab., Ariana, Tunisia

Habtamu Abie
Norwegian Computing Center, Oslo, Norway

Mieso Denko
University of Guelph, Ontario, Canada

Keywords: Smart sensor networks, Wearable and implantable sensors, Intelligent session management, Secure communication.

Abstract: The aim of Wearable and implantable monitoring devices is to collect relevant data from the application-related environment, and transmit this information to the outside world. Modern microelectronics create ever increasing opportunities, but it is still true that sensors form the weakest elements in the entire chain of data collection and processing. The difficulty of deploying smart body sensor networks is exacerbated by the hostile environments in which they are typically installed. In this paper, we propose a novel architecture for wearable and implantable body sensor systems that guarantees both real-time responsiveness and security. We rely on the wavelet packet transform to develop an intelligent session management scheme where a customizable frame structure allows multiplexing the set of sessions between the elementary sensors and the analysis center. We introduce a lightweight identity-based encryption protocol suitable for body smart sensor systems. We also present performance results using simulation experiments.

1 INTRODUCTION

The last decade has witnessed a rapid surge of interest in new sensing and monitoring devices for healthcare and the use of wearable/wireless devices for multiple applications (Puers, 2005). Key developments in this area include implantable in vivo monitoring, battlefield monitoring, and human tracking; where sensors are strategically placed at various locations on the vest or inside the human body to form a network (Body Sensor Network) and interact with the human system to acquire and transmit the data to an acquisition system. The data acquisition hardware collects the data from various sensors and transmits the processed data to the remote monitoring station.

The basic requirement for such systems is that the data gathered by the body sensors should be available for transmission in real-time in response to a query issued by the data acquisition system. When multiple sensors are involved in the measurement process, real-time responsiveness becomes hard to achieve since all sensor nodes share the same communication channel. Hence, the balance between response delay and scalability should be carefully addressed. In addition, security is a matter of concern in these networks, as the data being monitored are the health status of the individual. The sensor nodes used to form these networks are resource-constrained, which makes security applications a challenging problem. The data are also vulnerable to external attackers, who may inject errors in the routing information, replay old routing information, distort routing information or send malicious information. The data are also subject to jamming, tampering, Sybil attack, and collision (Hamdi and Boudriga, 2008. Attacks of this nature which have been thoroughly investigated and neutralized as threats within the context of traditional wireless sensor networks, still represent a threat to body sensor networks.

Hamdi M., Boudriga N., Abje H. and Denko M. (2010).
SECURE WEARABLE AND IMPLANTABLE BODY SENSOR NETWORKS IN HAZARDOUS ENVIRONMENTS.
In *Proceedings of the International Conference on Data Communication Networking and Optical Communication Systems*, pages 85-92
DOI: 10.5220/0002988200850092

In this paper we develop a secure network architecture for Wearable and Implantable Smart Sensor Networks (WISSNs). We first propose an architecture where intermediate sensor nodes allow the data collected by the elementary sensors to be forwarded to the analysis center (i.e., data acquisition center). To support this architecture, we propose a session multiplexing scheme that permits multiple elementary sensors to share the communication resources of an intermediate. It relies on wavelet theory since it is necessary to allocate a variable number of slots to a given elementary sensor in the multiplexed frames, the number of slots varying with the volume of date it generates or with its residual amount of energy. We propose, in addition, a security protocol addressing specific issues including authentication/anonymity, accounting, confidentiality, and investigation. The use of elliptic curve cryptography minimizes the power consumption of the cryptographic primitives while the absence of user information in the authentication protocol preserves privacy and anonymity.

The reader will notice that four innovative issues are addressed in this paper:

Layer-2 Multiplexing**:** Rather than being performed at the physical layer, the multiplexing of the information originating from multiple sensor nodes is dealt with using a specific frame structure based on the wavelet packet transform. Such multiplexing provides more fairness.

Real-time Responsiveness**:** The proposed architecture guarantees that the queries from the data acquisition center are processed in real-time by the smart sensor system since a set of intermediate sensors processes the information collected by the elementary sensors

Privacy/anonymity Provision**:** Our security protocol allows the data sent by the intermediate sensors to the analysis center to be enciphered using dynamic public keys. This guarantees the privacy of the collected data as well as the anonymity of the wearer.

Low Energy Consumption**:** The simulations that have been performed show that our cryptographic protocol is characterized by a low computational complexity, making it convenient for use with the limited resources of the intermediate sensors

The rest of this paper is organized as follows. Section II presents related work. Section III presents the WISSN. A novel session multiplexing technique based on wavelet theory is discussed in Section IV. Section V discusses security issues. Section VI provides validation and performance evaluation of the proposed techniques. And Finally, Section VII concludes the paper with suggested avenues of future research.

2 RELATED WORK

In recent years, there has been a proliferation of smart monitoring based on small sensing devices. A large portion of these devices have been devised for sports science and combating obesity. For instance, there are sophisticated watches available today (Polar), (Suunto) that provide real-time measurement of heartrate and allow athletes to store the gathered data on computers for further analysis using specific software. Bodymedia (BodyMedia) has developed an armband that has multiple sensors (galvanic skin response, skin and near-body temperature, two-axis accelerometer and heat flux) and collects physiological data on an on-going basis for days at a time. Once the data is uploaded to a computer, relevant and accurate information can be extracted about, for example, fatigue, duration of physical activity, consumed calories, etc. However, in all cases the physiological data is analyzed on a home PC at a later time, and proprietary data formats prevent users from consolidating and correlating health monitoring data from different devices.

In the medical domain, research is being conducted on the remote monitoring of physiological reactions (Scannell et al., 1995), (Martin et al., 2000), (Oliver et al., 2006). However, in existing approaches, as a rule no automated analysis is performed by the device, and the raw data is instead sent to a remote computer for further analysis by humans. Traditionally, personal medical monitoring systems, such as Holter monitors, have been used only to collect data for off-line processing. An exception to this is the approach proposed in (Oliver et al., 2006) where a cell phone is used to store, transmit (via Bluetooth) and analyze the physiological data, and present it to the user in an intelligible way. In (Leister et al., 2009) a security and authentication architecture using MPEG-21 for wireless patient monitoring systems has been developed based on the threat assessment of wireless patient monitoring systems. In (Leister et al., 2008), an architecture that can handle end-to-end management of multimedia content in diverse wireless sensor networks have been proposed.

Martin et al discuss in (Martin et al., 2000) the usage of wearable computers for health monitoring where the devices provide real-time feedback to the patient. In particular, they describe a wearable ECG device, but provide no experimental results. A wearable health-monitoring device using a Personal Area Network (PAN) or Body Area Network (BAN) can be integrated into a user's clothing (Park and Jayaraman, 2003), like Foster-Miller's health monitoring garment for soldiers. Along these lines, Paradiso (Paradiso, 2003) describes preliminary work on the WEALTHY system, a garment with embedded ECG sensors for continuous monitoring of the heart. Jovanov et al present in (Jovanov et al., 2005) a wireless BAN with motion sensors for computer-assisted physical rehabilitation and ambulatory monitoring. In (Kemp et al., 2008), Kamp et al develop a wearable system for manned bomb disposal missions. Mihovska and Prasad (Mihovska and Prasad, 2007) have developed an adaptive security architecture for personal networks with an asymmetric key agreement scheme on three levels by using contextual information, such as the location of the user and the capability of the devices. This architecture is based on an elliptic curve cryptosystem. It has, however, one shortcoming. It is susceptible to impersonation via key compromise.

A global notice about these approaches shows that traditional communication protocols are used to transmit the collected data from the human body to an external system (e.g., cellphone, laptop). Unfortunately, this does not guarantee a real-time transmission of this information since an important variable delay can occur, especially when some sensors transmit large units of data such as images. Moreover, due to the use of radio communication, the confidentiality of the transmitted data is not intrinsically guaranteed, which may lead to privacy violation. In several applications, including healthcare, even the identity of the wearer should be hidden.

3 PROPOSED WISSN ARCHITECTURE

In this paper, we address two crucial issues regarding wearable sensor systems:

•***Improving Real-time Responsiveness*:** This is achieved by building special communication frame structures based on the non-uniform multiplexing of the data generated by different types of sensors

•***Combining Sensor Authentication*** and user anonymity through the use of lightweight cryptographic protocols: In order to adapt to the severe resource limitations characterizing WISSNs, we use an elliptic curve implementation of the proposed security functions

In spite of its apparent simplicity, WISSNs exhibit several complex features and therefore require sophisticated engineering approaches in order to be set up. In the following, we list the most relevant factors that may shape the communication models used in smart sensor networks.

1. Multi-functional framework: A sensor node may be able to carry out multiple functions that can be set on/off depending on the situation. Obviously, the communication requirements may differ greatly from one functionality to another according to the data sent across the WISSN. For instance, when the network is deployed in a mining structure, a first category of sensor may be used to monitor the amount of several toxic gases in the atmosphere. A second type of sensor can serve to estimate the opacity of the encountered obstacles. IRM sensors can be used in such a context in order to predict, and possibly prevent, disasters. Since the volume of data generated by the latter category is by far greater than that generated by the former, much more bandwidth must be reserved to transmit image data.

2. Independent monitoring capability: Due to the non-uniform nature of the monitored events (irrespective of the application), some sensors may exhaust their energy more rapidly than others. This may result in the presence of uncovered regions where the nodes in charge of gathering data related to the environment are out of power. Since such a situation significantly affects the efficiency of the WISSN, solutions should be proposed to avoid it. One alternative is to tune the quality of the data gathered by a sensor node according to its residual energy resources. This would extend considerably the lifetime of this node at the cost of losing some refined data, which is definitely better than totally losing the functionalities provided by the node. As a result the communication resources required to transmit the data may vary from one sensor to another.

3. Exportable configuration: Configurations can be exported from one sensor to another in order to turn on/off several functionalities. Even though this feature allows energy to be saved (by triggering power-consuming time only when necessary), it creates a significant security hole since node imposture can be easily carried out. Hence, authentication mechanisms should be set up to prevent non-authorized nodes from manipulating the WISSN. Two important issues must be taken into consideration: First, the security algorithms must be based on non-complex algorithms and use small cryptographic credentials (to adapt to limited CPU time and memory resources) and; Second For a wide range of applications, the anonymity of the person holding the wearable or implantable smart sensor system should be preserved. Since this conflicts with authentication, specific security infrastructures will

have to be developed

From the foregoing discussion, it transpires that sessions on WISSNs should be managed bearing in mind that the specific features of such networks. In fact, a session should typically be initiated by a central external (i.e., not wearable) node, called the analysis center, in order to collect data from the WISSN. Henceforth, the underlying bandwidth management scheme should guarantee fairness for all body sensors. Unlike traditional networks, fairness in WISSNs should take into account the differences in the nature of the generated data and the available power level.

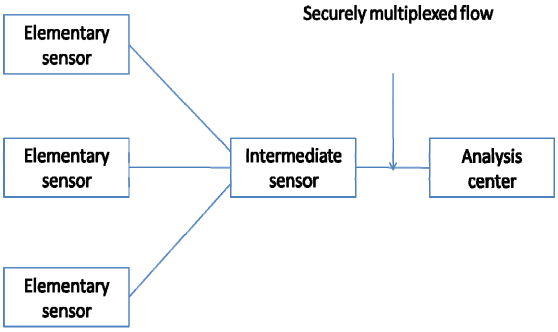

Figure 1: Wavelet packet decomposition.

Figure 1 illustrates this reasoning. In order to improve the scalability of the communication structure, we propose to divide the body area network into a set of clusters. We make the assumption that within each of these clusters, there is a central node which is in charge of forwarding the data gathered by the sensors present within the cluster and the analysis center. Since the contents of the frames sent out by the central node of a cluster to the analysis center originate from multiple body sensors, an intelligent multiplexing scheme is needed.

4 INTELLIGENT SESSION MANAGEMENT

This section develops a novel session multiplexing technique based on wavelet theory. We first discuss the mathematical aspects related to the wavelet packet transform. Then, we develop a multiplexing scheme where data emanating from multiple elementary sensors can be carried in a unique frame flow. For this purpose, we introduce a frame structure based on the parent-child relationship defined in wavelet theory. The Wavelet Transform (WT) is a time-scale transform that can be used to perform signal analysis. It offers effective time-frequency representation of signals. Wavelet theory and application have matured in recent decades and have proven to have tremendous application in fields such as data compression, multi-scale analysis, transient signal processing, and more. In practice, the wavelet transform is implemented using a couple of filters; a low-pass filter is used to generate approximation coefficients and a high-pass filter is used to generate detail coefficients. A decimation phase is also used so that the size of each of the approximation and detail signals is half the size of the input signal.

Mallat (Mallat, 1989) showed that a multi-resolution decomposition of a signal $f(t)$ can be achieved by iterating the wavelet decomposition on the approximation signal (which will be initialized to $f(t)$). More recently (Feil and Uhl, 1998), a more sophisticated multi-resolution analysis, based on the Wavelet Packet Transform (WPT), has been proposed to apply the wavelet transform to both the approximation and the detail coefficients at every decomposition stage. Figure 2 illustrates this transform where H_0 denotes the low-pass filter and H_1 denotes the high-pass filter.

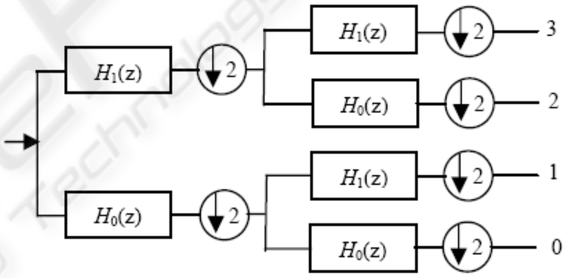

Figure 2: Wavelet packet decomposition.

For n levels of decomposition the WPT produces $2n$ different sets of coefficients (or nodes) as opposed to $(n + 1)$ different sets for the DWT. However, due to the downsampling process the overall number of coefficients is still the same and there is no redundancy.

The basic idea of our work is that larger time slots should be allocated to the sensor nodes that provide more refined data. For this purpose, we define a parent–child relationship between wavelet coefficients, and let the coarser resolution transport the most refined data. We have investigated dependencies between wavelet coefficients on this traffic. As shown in (Feil and Uhl, 1998), the dependencies between parent-child are very important. Therefore, the wavelet packet transform minimizes the cross-correlation between two decomposed signals. Therefore, a frame issued by an intermediate sensor node can carry data from multiple flows generated by different sensor nodes. This idea is detailed in the following.

Importance should be attached to the values on diagonals. The main diagonal is not so important in our case. More important are other diagonals, which directly show the dependencies between predecessors and successors. For example, second diagonal reveals direct parent-child dependency.

According to Figure 2, if the size of a signal *f*(*t*) is denoted by *s*, then the size of the signals obtained after *n* wavelet stages is *s*/2*i* (the rounding operator is omitted because we suppose that *s* is a power of 2). Therefore, if n is the number of elementary sensors and *F* is the frame size; then, a fair decomposition of the frame gives that <F/n> bits are allocated to every elementary sensor, where <.> denotes the rounding operator. Hence, the frame can be structured so that the analysis center reconstructs the signals corresponding to lower decomposition depths before those corresponding to deep depths. The role of the intermediate sensor is simply to increase the depth of the wavelet packet transform according to the priority of the corresponding sensor node.

5 SECURITY PROTOCOL

The first step in ensuring secure data aggregation at intermediate nodes is to enable the intermediate nodes to have appropriate encryption/decryption keys to communicate and decipher the incoming data, apply the aggregation function and relay them forward. When data is relayed, it is assumed that it is broadcast (using omni-directional antenna). Furthermore, if the same data has to be transmitted to several nodes and if the nodes are operating using distinct pair-wise keys, then, care must be taken to transmit the data multiple times, each time encrypted differently with a different key. This could potentially be a drain on energy and a hindrance to in-network processing. As we have seen earlier, having a common key for the group of nodes is a possible solution to this problem, but has an inherent weakness in that the whole network could be compromised if an attacker successfully attacks any one node.

The basic idea behind our protocol is to make a sensor independently generate a public key using an arbitrary string. For example, a sensor collecting data of type *T* at time *t* will first create a string σ = (*sensor_id*|*t*|*T*). Using this string, the sensor can derive a public key, π_σ to encrypt the data and send them to the storage site. There is no corresponding secret key created. In fact, the sensor cannot create the secret key needed to decrypt the message.

When the sensor wishes to release this information to the analysis center, the sensor can derive the corresponding secret key, κ_σ, by using the same string σ. This secret key only allows the analysis center to decrypt messages encrypted by a sensor using the same string. This simplifies key management, since the sensor can generate the secret key on-demand without keeping track of which keys were used to encrypt which data. The only requirement is that the string used to describe the event is the same.

Setup: We select an elliptic curve *E* over *GF*(*p*), where *p* is a big prime number. We also denote *P* as the base point of *E* and *q* as the order of *P*, where *q* is also a big prime. A set of *n* secret keys $\kappa_1,\dots,\kappa_n \in GF(q)$ is chosen to generate the master secret key, denoted by $K = (\kappa_1,\dots,\kappa_n)$. The *n* public keys are then generated to make up the master public key, denoted by $\Pi = (\pi_1,\dots,\pi_n)$, where $\pi_i = \kappa_i.P$, $1 \le i < n$. Finally, a collision resistant one-way hash function is chosen,

The parameters (Π, *P*, *p*, *q*, *h*(.)) are released as the system public parameters.

Keygen: To derive a secret key κ_σ corresponding to a public key generated by a string σ, the sensor executes ***keygen***(σ) = κ_σ,

$$\kappa_\sigma = \sum_{i=1}^{n} h_i(\sigma).x_i,$$

where $h_i(\sigma)$ is the *i*-th bit of *h*(σ).

Encrypt: To encrypt a message m using a public key derived from string σ, the sensor does ***encrypt***(*m*,σ) to determine the ciphertext *c*.

```
Algorithm encrypt
Determine string σ using agreed-upon syntax
  Generate public key $\pi_\sigma$ where
            $\pi_\sigma = Pn_i=1\ h_i(\sigma) \cdot yi$
Execute EccEncrypt(m, $\pi_\sigma$) to obtain c
```

Decrypt: The analysis center executes ***decrypt***(*c*, κ_σ) to obtain the original message m which was encrypted using a secret key derived from σ.

```
Algorithm decrypt
Requests permission from sensor to obtain data described by σ
Sensor runs Keygen(σ) to derive $\kappa_\sigma$
Analysis center executes EccDecrypt(c, $\kappa_\sigma$) to obtain m
```

Based on these functions, we develop the following protocols for secure data collection, transfer, and aggregation.

Secure Data Collection: Having collected an event d, the sensor executes the following algorithm to encrypt it.

```
Algorithm secure_data_collection
    Derive the string $\sigma$, and generate a random number n
    Calculate m1 = (flag|n) where flag is a known bitstring
    Calculate m2 = (d|n)
    Calculate c1 =Encrypt($\sigma$,m1)
    Calculate c2 =Encrypt($\sigma$,m2)
```

Secure Data Transfer: Periodically, each sensor in the WISSN will transfer its data to the analysis center. This is done by first aggregating all the data into an intermediate sensor node, which then forwards the aggregated data to the storage site. Assuming that there are k tuples generated by the WISSN, the intermediate sensor will forward the set $\{(c_{11}, c_{12}), \dots, (c^k_1, c^k_2)\}$.

Secure Data Querying: An analysis center wishing to obtain data collected under some σ will first contact the CA for permission. After the CA agrees, the CA will run Keygen(σ) to derive the corresponding secret key κ_σ needed to decrypt data. Then, the following algorithm is executed to decrypt the data:

```
Algorithm Secure data querying
for every ($c^i_1$, $c^i_2$) i $\in$k for sensor do
    Storage site sends ci1 to analysis center
    Analysis center runs Decrypt($c^i_1$, $\sigma$)
    if the initial bits of the result match flag then
            Analysis center requests corresponding $c^i_2$ from storage site
            Analysis center executes Decrypt($c^i_2$, $\sigma$) and checks whether the n matches the value from $c^i_1$
        Analysis center accepts d if both are correct
    end if
end for
```

Since all the data are encrypted, the storage site cannot return a specific encrypted tuple to the analysis center. Instead, the storage site simply lets the analysis center try to decrypt each tuple (c_1, c_2) belonging to the sensor. The reason for returning c_1 to the analysis center first instead of returning c_2 directly is to improve efficiency. Since the length of c_1 is much shorter than c_2, letting the analysis center first attempt to decrypt c_1 before sending the much longer c_2 reduces transmission time.

The analysis center can check if the data obtained from the storage site belongs to his sensor by checking whether the same random number n is used in both c_1 and c_2. Since this random n is known only to the sensor encrypting the data, only that sensor can embed the same n in both c_1 and c_2.

6 ASSESSMENT AND EVALUATION

In this section, we validate the proposed session management and security protocols. We first analyze the features of the developed functionalities with respect to the requirements given in Section III. Then, we proceed to a performance evaluation based on simulation of the wavelet-based session management scheme. Finally, we discuss the security properties guaranteed by our cryptographic protocols.

A. *Proving Features*

We discuss the features of the developed functionalities with respect to real-time responsiveness, fairness, privacy and anonymity.

***Real-time responsiveness*:** The data acquisition center is able, via structured queries, to have the data collected by the sensor nodes nearly in real-time. In fact, the period between two queries has to be sufficient for the transmission of *n.l.p.s* bits, where n is the number of elementary sensors, l is the event rate, p is the even gathering periodicity, and s is the average signal size. For n=10, l=2, p=1mn, and $s=2^9$, we find that the transmission rate between the elementary sensor and the analysis center should be approximately 6kb to fulfill the real-time requirement. The period of time needed to upload all the collected events to the analysis center would be 0.6 seconds, in that case, using a 10kb/s link.

***Fairness*:** the allocation scheme used when building the upward frame guarantees an equal slot of time for all nodes constituting the BAN. Nodes that have larger quantities of information to send are provided with greater depth, using wavelet transform, to send more data in the same period of time. This approach reduces the latency measured for the arriving data at the analysis center.

***Privacy and Anonymity*:** privacy provided by a BAN in a hazardous environment covers personal information related to the wearer and information related to the collecting sensors (e.g., used algorithms and nature of the data collected). After multiplexing the collected data, the transmitted frame is unable to show any of the private information since the wavelet transform will mix these data at variable depths. In addition, a public encryption is added to this process.

B. *Security Evaluation*

The main overhead of our protocols is the amount of time needed to generate a single π_σ from a string σ using n number of public keys $\pi_1, \dots, \pi_n$. Note that the value of n is not related to the number of different π_σ s that can be generated. The WISSN can continue to generate as many π_σ on-the-fly as needed, regardless of the value of n. Once π_σ is generated, the remaining encryption is the same as that for a regular ECC encryption.

Figure 3 shows the amount of time needed to generate a single π_σ with varying values of n. All n public keys are initially stored in the flash memory. Figure 4 shows the amount of flash storage need to store *n* different public keys. We see from Figure 3 that, for $n = 360$, we need only 0.9 seconds to generate π_σ.

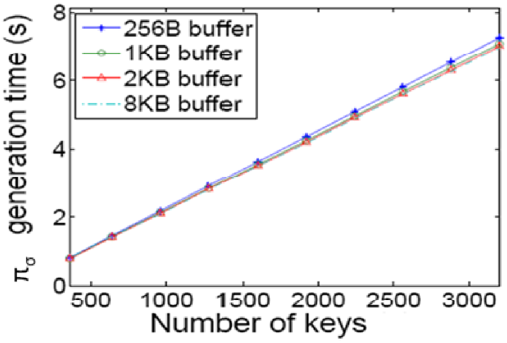

Figure 3: Time needed to derive one public key versus the number of elementary keys.

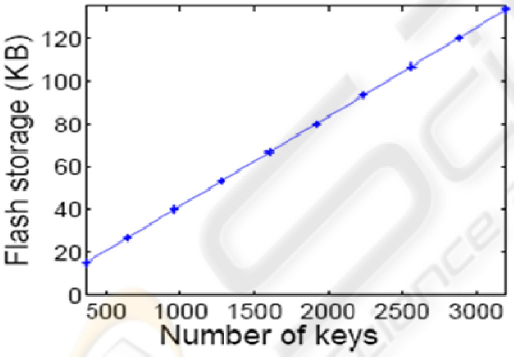

Figure 4: Flash memory storage needed to store one public key versus the number of elementary keys.

Figure 5 shows the time needed to perform the encryption once the public key π_σ has been derived. For a given piece of data, encrypting with just one π_σ requires about 1.5 seconds. Again this is the encryption time for the symmetric key (r), which will then be used to encrypt the raw data. The symmetric key can be used for a period, say 10 minutes. The cost of the 1.5s can be compensated over the 10 minute period. The amount of time needed for multiple π_σs to encrypt the same data is proportional to the number of π_σs. While in Figure 5 the amount of time needed for 10 different π_σ is close to 15 seconds while it is worth mentioning that ,in practice, we are unlikely to use many different public keys to encrypt the same event.

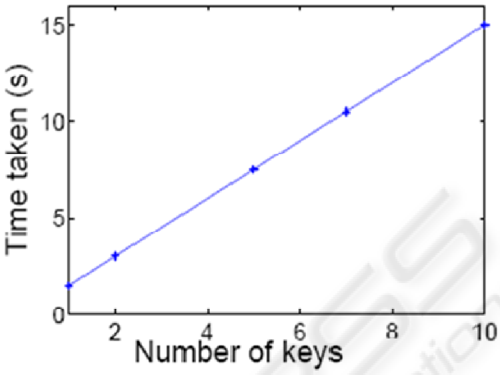

Figure 5: Time needed for encryption versus number of keys.

7 CONCLUSIONS AND PERSPECTIVES

In this paper, we defined an architecture for secure wearable and implantable smart sensor networks where an analysis center periodically launches queries to gather data related to the monitored environment. To adapt to the hazardous nature of the contexts where such systems are typically deployed, we proposed a multiplexing scheme and a cryptographic protocol based on wavelet packet decomposition and elliptic curve cryptography respectively. We have shown that these approaches provide real-time responsiveness (through intelligent session management) as well as anonymity (since the human identity is not involved in the cryptographic protocol).An extension of the session multiplexing technique to a physical layer is under development for use in situations where the optical sensors are linked to the analysis center via laser beams. Moreover, a simpler security protocol not involving intervention by the certification authority is being developed.

Our future work will also include the design and deployment of wearable and implantable smart sensor nodes with light-weight self-abilities to detect in real time unknown activity patterns, to swiftly respond to them, and to learn activity patterns over time and adapt to the dynamism of the hazardous environment and to changing degree of security and privacy breaches. Such abilities may enable the reduction of communication overhead between nodes. Applications scenarios such as healthcare and smart homes will be investigated.

REFERENCES

Robert Puers, "Implantable sensor systems", DISens symposium- book 2005.

M. Hamdi, N. Boudriga, "Security In Wireless Sensor Networks," Handbook of Research on Wireless Security, Information Science Reference, ISBN-10: 159904899X, March 2008.

Polar. Polar watches. http://www.polarusa.com.

Suunto. T6, foot pod, n6hr. http://www.suunto.com.

BodyMedia. Healthwear armband, bodybugg. http:// www.bodymedia.com.

K. M. Scannell, D. A. Perednia, and H. M. Kissman. Telemedicine: Past, present, future. Technical report, U.S. Department of Health and Human Services. National Library of Medicine. Reference Section., 1995.

Martin. T., E. Jovanov, and Raskovic. D. Issues in wearable computing for medical monitoring applications: A case study of a wearable ecg monitoring device. In Proc. Intl. Symp. Wearable Computers (ISWC'00), pages 43–49, 2000.

Oliver, N. Flores-Mangas, F. HealthGear: a real-time wearable system for monitoring and analyzing physiological signals. International Worskhop on Wearable and Implantable Body Sensor Networks, 2006.

S. Park and S. Jayaraman. Enhancing the quality of life thourgh wearable technology. IEEE Engineering in Medicine and Biology Magazine, 22:3:41–48, 2003.Dfd

R. Paradiso. Wearable health care system for vital signs monitoring. In Proc. IEEE Int. Conf. Information Technology Applications in Biomedicine, pages 283–286, 2003.

E. Jovanov, A. Milenkovic, C. Otto, and P. C. de Groen. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. Journal of Neuroengineering and Rehabilitation, 22:6, 2005.

Kemp, J., Gaura, E. I., Brusey, J. 'Instrumenting Bomb Disposal Suits with Wireless Sensor Networks.' In Proceedings of the 5th International Conference on Informatics in Control, Automation and Robotics (ICINCO 2008). May 11-15 2008 at Funchal, Madeira – Portugal, 2008.

S. G. Mallat "A Theory for Multiresolution Signal Decomposition : the Wavelet Representation",. IEEE PAMI, Vol.11(7), pp.674−693, 1989.

M. Feil and A. Uhl. Wavelet Packet Decomposition and Best Basis Selection on Massively Parallel SIMD Arrays. Proceedings of the International Conference "Wavelets and Multiscale Methods" (IWC'98), Tangier, 1998.

A. Mihovska and N. R. Prasad, Adaptive Security Architecture based on EC-MQV Algorithm in Personal Network (PN), Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous 2007), Volume, Issue, pp. 1-5, 6-10 August, 2007

W. Leister, H. Abie, A.-K. Groven, T. Fretland and I. Balasingham, "Threat Assessment of Wireless Patient Monitoring Systems," ICTTA'08 (Intl. Conf. on Information and Communication Technologies: From Theory to Practice), Damascus, Syria, 7-11 April 08, 2008.

W. Leister, T. Fretland, and I. Balasingham, Security and Authentication Architecture Using MPEG-21 for Wireless Patient Monitoring Systems, International Journal on Advances in Security, 2009 Vol. 2, No. 1 (in press)