BARI: A Distributed Key Management Approach for Wireless Body Area Networks

Syed Muhammad Khaliq-ur-Rahman Raazi,
Sungyoung Lee, Young-Koo Lee
Ubiquitous Comp. Lab., Dept. of Comp. Engg.
Kyung Hee University(Global Campus)
Yongin, Korea
E-mail:raazi@oslab.khu.ac.kr,
sylee@oslab.khu.ac.kr, yklee@khu.ac.kr

Heejo Lee
Divison of Computer & Comm. Engg.
Korea University
Seoul, Korea
E-mail: heejo@korea.ac.kr

***Abstract*—In recent years, use of sensors to measure the biometrics and movements of human body have resulted in the design of wireless body area networks (WBAN). Although WBANs consist of resource constrained sensing devices just like other wireless sensor networks (WSN), they differ from WSNs in topology, scale and security requirements. Due to these differences, key management schemes designed for WSNs prove inefficient and unnecessarily complex when applied to WBANs. Considering key management issue, WBANs are also different from WPANs because WBANs can use random biometric measurements as keys. We highlight the differences between WSN and WBAN and propose an efficient key management scheme, which makes use of biometrics and is specifically designed for WBANs domain.**

***Keywords*-Humanware; Wireless Body Area Networks; Key Management; Biometrics; Security.**

I. Introduction

A. Background

Sensor networks are used to monitor chemical, biological, physical, environmental or any other kind of phenomena in real-time environments. Sensor networks consist of resource constrained sensor devices, which relay their sensed data to a central server through the network using wireless communications [1]. This data is processed or used at the central server according to the application requirements. In order to increase efficiency, information is also filtered in the intermediate nodes [2].

A wireless body area network (WBAN) is formed when sensor nodes are tactfully placed on human body to collect its biometrics or activities. Applications of WBAN include healthcare, lifecare and athlete examination. Healthcare includes care for inpatients especially those who are seriously ill, unconscious or under intensive care. Lifecare includes patients, who live their lives normally but may require medical care at any time. For example, lifecare facilities are useful in monitoring health of elderly people and pregnant women in real-time. Lack of timely medical care may cost some people their lives e.g. heart patients or high risk pregnant women. Also, WBANs are very useful in examining and monitoring an athlete's body.

The use of WBAN in applications, which are crucial for human life, highlights the importance of its security. Apart from making sure that a person's biometric information is not tampered with, we also need to ensure confidentiality of the person's information. Key management plays a pivotal role in ensuring data integrity and protecting patient's private data from eavesdroppers and unauthorized users.

In order to ensure confidentiality and integrity, highly secure state-of-the-art mechanisms such as TLS [3] and Kerberos [4] exist but they are too heavy to run on resource constrained sensor nodes. Mechanisms such as LEAP+ [5], SHELL [6] and MUQAMI [7] are resource efficient for sensor nodes but they are designed keeping in mind unattended large scale Wireless Sensor Networks (WSN), in which all nodes may not be in communication range of each other. Apart from being small scale wireless network that can have human intervention, WBAN have all nodes in communication range of each other. Also, we can exploit the application characteristics of WBAN to further reduce the key management overhead. Differences between WSN and WBAN are discussed in detail in the following section (Section I-B).

B. Motivation and Problem Statement

WBANs are adhoc networks formed by the sensor nodes placed on different parts of a human body. Sensor nodes have less memory, computation and communication capabilities. Also, they have limited energy resources. Based on the above properties, WBANs are classified into the same category as WSNs and thus treated the same way, when designing schemes for key management. However, we find that WBANs are different from usual WSN in many ways.

Firstly, WBANs and WSNs differ in scale. For WSNs, number of nodes may be in thousands while WBANs consist of a very few nodes, which may not exceed twenty. Obvious reason for this difference is usability. In humanware applications, sensor devices can be placed in watches, lockets or other wearable things. People may not agree to wear a lot of devices. If they do, it will hamper their daily routine.

Secondly, nodes in WBANs are very close to each other as opposed to WSNs. Nodes in WSNs are scattered in large areas like battlefields while nodes in WBANs are placed in a small area i.e. a human body. This renders all the nodes in WBANs in communication range of each other unlike WSNs. Communication protocols have been designed keeping in mind such topology [8].

Thirdly, a compromised node can be physically removed in WBAN, which may not be the case in WSN because human intervention is not always possible in WSNs. In applications of WBAN, which are crucial for human life, it is essential to physically replace a compromised node. For example, if there is only one node measuring a serious patient's heart rate, it must be replaced immediately. Since it is possible to physically remove a compromised node in WBANs, it is not efficient to include node eviction strategies in key management scheme.

Lastly, WBANs are used to measure biometrics from a human body. Biometrics exhibit sufficient randomness properties to be used as cryptographic keys. Phenomena measured in a WSN application may not have such characteristics. Due to such application characteristics, WBAN can not be treated as a Wireless Personal Area Network (WPAN) too. Some researchers have used biometrics for key generation [9],[10]. Some researchers argue that sensor nodes do not even need to exchange keys [11],[12],[13]. They rely on the assumption that two nodes can sense a biometric at the same time. Then they apply error-correcting codes at both the communicating nodes. Apart from extra computations and time synchronization issues, this assumption imposes another constraint on the network i.e. Some nodes should be able to sense more than one biometric, which may not be practically possible. Also, such schemes do not take into account those nodes, which are not used for sensing biometrics. For more detail, refer to the system model described in Section III.

We have summarized the differences between WBAN and WSN in table I. The only difference in security requirement of WBAN and WSN evident from table I is that a compromised node in WBAN scenario need not be evicted through software because human intervention is always possible. However, there is also a difference between types of attack that can take place through a compromised node in WBAN and WSN scenarios. In WBAN, we don't need to take care of routing attacks such as selective forwarding, wormhole and sinkhole attacks because all nodes have the cluster head in their communication range. Moreover, due to the fact that WBAN are small scale networks, in which all nodes are in communication range of each other, we don't need to employ strategies to prevent attack propagation in WBAN. Also, we can achieve more efficiency in key management solutions if we exploit the characteristics of WBAN applications while designing key management scheme for WBANs.

Table I
DIFFERENCES BETWEEN WBAN AND WSN

	WBAN	**WSN**
Scale	Small scale (Number of nodes may not exceed 20)	Large scale (Number of nodes may exceed even 1000)
Size of Operational Area	Very small (Size of human body). All nodes may be in communication range of each other	Spans large area like battlefields or natural habitat
Human Intervention	Possible rather inevitable in some cases	Not possible in most cases
Key Management Support from application	Yes, Sensor nodes need not generate random numbers	No

C. Main Contributions

In this paper, we present BARI, which is a distributed key management scheme that fulfills the security requirements of WBAN and also exploits the application characteristics of WBAN to achieve more efficiency.

Rest of this paper is organized as follows: Section II outlines the related work followed by section III, which states the system model and assumptions. Section IV presents our scheme. Section V presents simulation results and then section VI concludes the paper.

II. RELATED WORK

Due to the fact that WBAN consist of sensor nodes, they have been considered similar to WSNs. Therefore, most of the related work is from the WSN paradigm. The most simple key management solutions is to distribute keys to each pair of communicating nodes before the deployment and then use them throughout the network lifetime. Extreme care must be taken during key assignments otherwise it may result in inefficient security. For example, same key should not be assigned to multiple pair of nodes within a certain area. Likewise, there are many other issues in key pre-distribution. Efficient mechanisms, which take care of those issues, also exist [14],[15]. However, if we keep using same keys for longer periods of time, they may come under cryptanalytic attacks. In WBAN, network lifetime may be indefinite because nodes' batteries can be replaced or recharged. Under such circumstances, periodic key refreshment becomes necessary.

Many schemes, which support key refreshment, have been proposed for WSN. LEAP+ [5] is a localized key management scheme and one of the state-of-the-art solution for WSN. Common drawback of LEAP+ is their assumption regarding network safety during some initial time period. Also, LEAP+ is not designed for a scenario, in which all nodes are in communication range of each other. Apart from that, SHELL [6] and MUQAMI [7] are lightweight solutions and suit the resource constrained sensor nodes well. Both these schemes are based on combinatorics and Exclusion Basis System (EBS) matrix [16]. MUQAMI improves the performance by distributing the key management responsibilities locally. Also, it makes use of key-chains [17], which are based on Lamport's one-time passwords [18]. However, both these schemes are designed keeping in mind the large scale nature of WSN. When applied to small scale networks, their performances drop considerably. Also, EBS based key management schemes are prone to collusion attacks [19].

All of the above schemes are generally efficient in WSN scenarios but none of them makes use of the characteristics of a WBAN application. Also, their designs are overly complex for WBAN scenario. Some researchers have focused on the application characteristics of WBANs but their research has been limited to the usage of measured biometrics as keys and authentication codes [9],[10],[11],[12],[13] as already discussed in Subsection I-B. We have proposed a complete key management architecture keeping in mind the application characteristics and security requirements of WBANs. To our knowledge, this is the first time a key management scheme is proposed keeping in mind the application characteristics and security requirements of WBANs.

III. System Model and Assumptions

Scenario of a WBAN is such that there are a few sensor devices, which are capable of measuring biometrics related to human body. These devices are tactically placed on a human body in such a way that they do not hamper the daily routine of the human being. Also, there is a Personal Server (PS), which can be a laptop or a hand held device. The PS and all the sensor nodes form a wireless body area network (WBAN). Sensor nodes measure the biometrics and forward the body related information to the PS. In turn, the PS relays this information to a central server, which we call a Medical Server (MS), through the internet.

Each WBAN is associated with only one body. Multiple WBANs are associated with one central MS. The MS stores and processes information of all the WBANs that are associated with it. An application software running on the MS generates alerts based on the information stored on the server. Also, authorized people can access the required information from the MS. System architecture, as per our assumptions, of WBAN is shown in Figure 1.

We assume that the PS and all sensor devices are constrained in energy because they use rechargeable batteries.

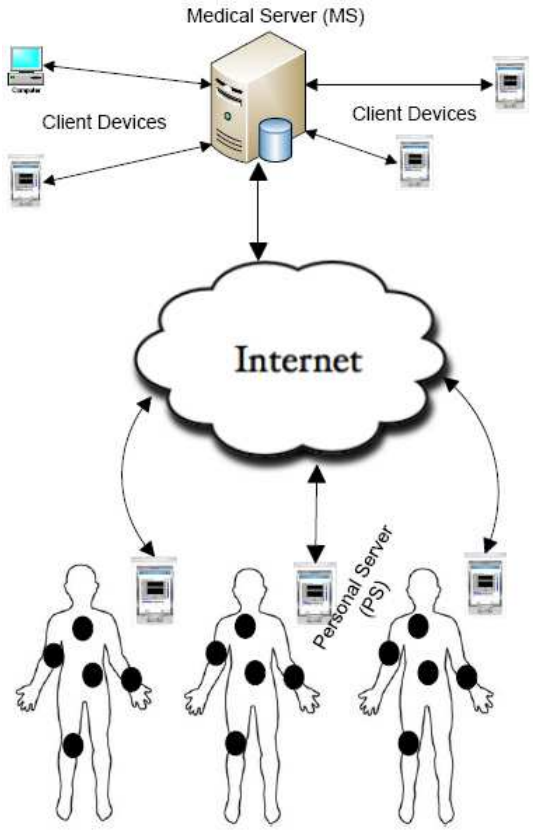

Figure 1. System Architecture of Wireless Body Area Networks

Unlike other WSN, physical node capture is not possible in WBAN because all nodes are under human observation. However, confidentiality, message integrity and node authenticity need to be taken care of.

IV. BARI

Our scheme supports the use of biometric measurements as symmetric keys because they posses the properties of random numbers and have been used as symmetric keys in WBAN previously. Our scheme makes use of key refreshment schedule, which depict the turn of each node for key refreshment. The personal server (PS) issues new key refreshment schedule periodically. Each node refreshes the key in the slot allotted to it.

Our scheme uses three types of keys to manage a WBAN: communication key, administrative key and basic key. Among the three types of keys, communication key K_{comm}, which is a network wide key and managed by the PS itself, is used to transfer data through the network in a secure manner. K_{comm} must be refreshed regularly to prevent cryptanalytic attacks.

Administrative key K_{admin}, which is also shared by multiple nodes, is used to refresh K_{comm}. K_{admin} is not used as frequently as K_{comm} so there is less probability that it comes

under cryptanalytic attack. We use refreshment schedules to distribute the responsibility of key management evenly throughout the network. In order to increase resilience in a WBAN, we can increase the number of administrative keys being used.

In WBAN applications, it is nearly impossible for an adversary to compromise a node physically or to place a malicious node nearby because of possible human intervention. Even if such an event occurs, it is a lot easier to detect and rectify. In order to cater for rare circumstances, we employ basic keys K_{bsc} in our key management framework. Every node has its own K_{bsc}, which it shares with the MS and is not known to any other node in the network. Also, K_{bsc} is used to refresh K_{admin} in case it is compromised.

A. Initial Deployment

In the first phase, PS is deployed. The PS comes pre-loaded with K_{admin}, K_{comm}, identities and authentication codes of all the nodes that are to be deployed in the network. When the PS is up and running, sensor devices are deployed on various parts of the body. Sensor nodes come pre-loaded with K_{admin} and their respective K_{bsc}. Soon after deployment, every node sends discovery message to the PS as follows: -

$$m1\text{: } \forall i \quad if \exists SN^i : SN^i \rightarrow PS : E_{K_{admin}}\{ID|Auth\_Code\}$$

After all the sensor nodes are deployed, the PS generates a key refreshment schedule for K_{admin} and then broadcasts it with the initial value of K_{comm}: -

$$m2 : PS \rightarrow * : E_{K_{admin}}\{K_{comm}|Key\_Ref\_Schedule\}$$

As soon as the last expected node's discovery message is received or a timer expires, the PS calculates the refreshment schedule and broadcasts its initial message $m2$.

B. Re-keying

In order to refresh K_{comm}, the PS selects suitable value of a biometric as the value of new K_{comm}. It then encrypts the new value of K_{comm} with K_{admin} and broadcasts it into the network as follows: -

$$m1 : PS \rightarrow * : E_{K_{admin}}\{K_{comm}\}$$

Administrative key is refreshed periodically. When the turn of sensor node i arrives, sensor node i waits for a certain period of time, chooses a suitable value of a biometric as new value for K_{admin} and broadcasts it into the network as follows: -

$$m1 : SN^i \rightarrow * : E_{K^{old}_{admin}}\{K^{new}_{admin}\}$$

When the key refreshment schedule expires, the PS calculates the new schedule, encrypts it in the current value of K_{admin} and broadcasts it into the network as follows: -

$$m1 : PS \rightarrow * : E_{K_{admin}}\{Key\_Ref\_Schedule\}$$

Sometimes, administrative key needs to be refreshed out of schedule. If it is the turn of sensor node i to refresh the administrative key, following messages will be exchanged to refresh K_{admin} out of schedule: -

$$m1 : PS \rightarrow SN^i : E_{K_{admin}}\{Key\_Refresh\_Msg\}$$

$$m2 : SN^i \rightarrow * : E_{K^{old}_{admin}}\{K^{new}_{admin}\}$$

In some rare circumstances, we may need to refresh K_{admin} through K_{bsc}. In such scenario, PS will ask the MS to refresh K_{admin} using K_{bsc}. MS will encrypt a new value of K_{admin} in K_{bsc} of all the sensor nodes. Then it will send these values to the PS. Also, MS will send the new value of K_{admin} to the PS. After that, PS will just forward the encrypted values of K_{admin} to the respective sensor nodes as follows: -

$$m1 : \forall i \quad if \exists SN^i : PS \rightarrow SN^i : E_{K^i_{bsc\_old}}\{K_{admin}|K^i_{bsc\_new}\}$$

$$m2 : PS \rightarrow * : E_{K_{admin}}\{K_{comm}\}$$

Remaining key refreshment schedule is followed after the refreshment of K_{admin} irrespective of the way K_{admin} is refreshed.

C. Node Addition

In some cases, new nodes are added to the network or the existing nodes are replaced. One possible scenario of node addition can be the deployment of a new device to monitor some biometric. Similarly, one possible scenario of node replacement is malfunction of a device. Under such circumstances new nodes are added to the network.

If a new node is to be added to the network, MS informs PS about new deployments by sending identities and authentication codes of new nodes to the PS. MS also informs the PS about the initial value of K_{admin} that is preloaded into the new nodes. All this communication is done through the internet or some other external channel. Under normal circumstances the PS ignores messages from stranger nodes and report a malicious activity. If informed by the MS, the PS expects discovery messages from new nodes. New nodes send their respective discovery messages encrypted in the pre-loaded value of K_{admin} as follows: -

$$m1 : \forall SN^j \in \{New\_Nodes\} : SN^j \rightarrow PS : E_{K^{pre-load}_{admin}}\{ID|Auth\_Code\}$$

Just like in the initial deployment phase, PS waits for all the expected nodes for a certain period of time. After that, it broadcasts the remaining key refreshment schedule and current values of K_{comm} and K_{admin} to the newly deployed nodes as follows: -

$$m2 : PS \rightarrow * : E_{K^{pre-load}_{admin}}\{K_{comm} |K_{admin}|Remaining\_Sched\}$$

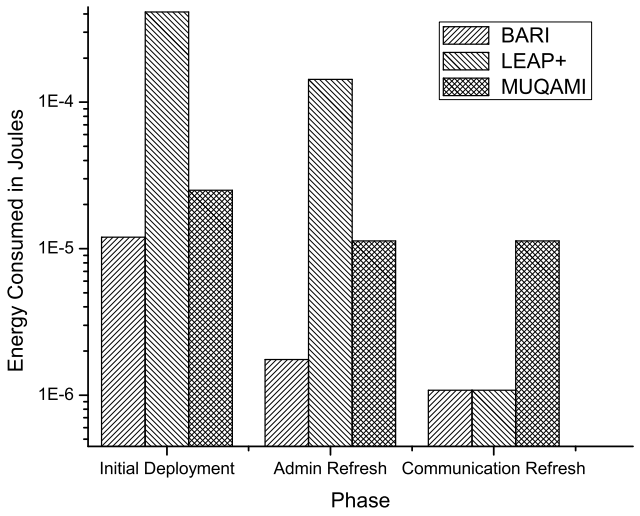

Figure 2. Comparison of Average Energy Consumed by a sensor node in different phases of each scheme

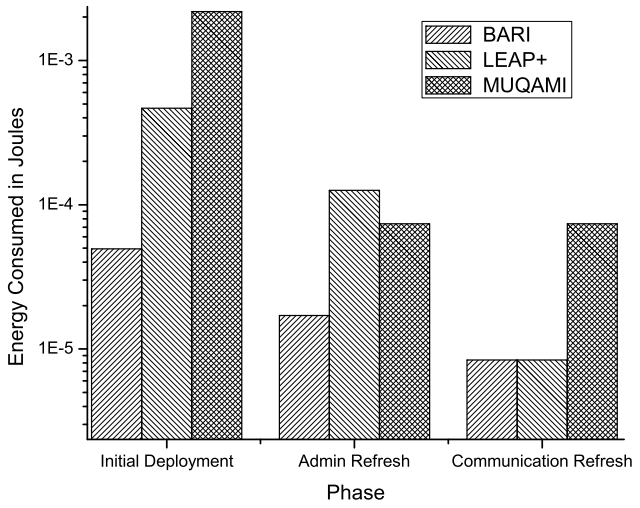

Figure 3. Comparison of Average Energy Consumed by a personal server in different phases of each scheme

Newly deployed nodes participate in the key refreshment procedure after the next key refreshment schedule is issued by the PS.

Security Analysis: Like other schemes, our scheme provides basic protection i.e. it helps maintain confidentiality, authenticity and integrity of information. In addition to that. we must consider different types of attacks that can take place in WBAN scenario. Since most of the related work in in WSN domain, we will consider attacks that can occur in WSN, then see if they are applicable in WBAN domain and whether our scheme provides adequate protection against them or not.

In WBAN, it is not a requirement to guard against attacks that involve routing. This is due to the fact that all nodes are in communication range of each other. Our scheme provides adequate protection against outsider attacks because member nodes ignore all communications from stranger nodes except during the phases of initial deployment and node addition. Even in these phases, only those nodes are entertained, which provide valid authentication code encrypted in a valid cryptographic key. Although an insider attack is not very likely to take place due to possible human presence and possible human intervention, our scheme provides protection mechanism using sensor nodes' basic keys.

V. Simulation Results

In our simulation, we have compared our scheme with two state-of-the-art schemes for WSN MUQAMI [7] and LEAP+[5]. For MUQAMI, we have assumed $k = m = 4$ and key-chain length to be 32. Number of sensor nodes is assumed to be 15 and key size is assumed to be 16 bytes in our simulation. Simulation was programmed in "Tools Command Language (tcl8.0)", which is used to program ns-2 simulations.

Our scheme uses biometrics as keys and need not generate them but other schemes are not designed to take full advantage of this property of WBANs. Costs of key generation, communication and computation were calculated as in [20]. With the above set of simulation parameters, we recorded the average energy consumed by PS and SN nodes during initial deployment phase, administrative key refreshment phase and communication key refreshment phase multiple times. Figures 2 and 3 compare the average energy consumed by a SN node and a PS node respectively in each of the three schemes in all three phases. Our scheme proves to be more efficient than MUQAMI in all the three phases and better than LEAP+ in initial deployment and administrative key refreshment phase.

VI. Conclusion and Future Work

We have highlighted the differences between WSN and WBAN in terms of application characteristics and security requirements. After that, we presented BARI, which is a key management scheme designed specifically for WBAN applications. BARI provides required level of security in WBAN while exploiting the application characteristics of WBAN, which other schemes are unable to do. Also, we have provided presented simulation results to prove our claim. In future, we plan to extend this work by providing detailed analysis of our scheme and its comparison with other schemes in terms of storage, computation cost, communication cost and the security features it provides.

Acknowledgment

This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised

by the IITA(Institute of Information Technology Advancement)" (IITA-2009-(C1090-0902-0002)) and Was supported by the IT R&D program of MKE/KEIT, [10032105, Development of Realistic Multiverse Game Engine Technology]. This work also was supported by the Brain Korea 21 projects and Korea Science & Engineering Foundation (KOSEF) grant funded by the Korea government(MOST) (No. 2008-1342).

REFERENCES

[1] S. Tilak, N. Abu-Ghazaleh, and W. Heinzelman, "A taxonomy of wireless microsensor network models," *ACM Mobile Computing and Comm.*, vol. 6, no. 2, pp. 1–8, 2002.

[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[3] T. Dierks and C. Allen, "The tls protocol version 1.0," United States, 1999.

[4] J. Kohl and C. Neuman, "The kerberos network authentication service (v5)," United States, 1993.

[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sen. Netw.*, vol. 2, no. 4, pp. 500–528, 2006.

[6] K. Ghumman, "Location-aware combinatorial key management scheme for clustered sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 17, no. 8, pp. 865–882, 2006, senior Member-Younis,, Mohamed F. and Senior Member-Eltoweissy,, Mohamed.

[7] S. M. K. Raazi, A. M. Khan, F. Khan, S. Lee, and Y. Song, "MUQAMI: A locally distributed key management scheme for clustered sensor networks," in *Trust Management*, ser. IFIP International Federation for Information Processing, vol. Volume 238/2007. Springer Boston, 2007, pp. 333–348.

[8] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *Journal of Mobile Multimedia*, vol. 1, no. 4, pp. 307–326, 2006.

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

[10] S. Cherukuri, K. K. Venkatasubramanian, and E. K. S. Gupta, "BioSec: A biometric based approach for securing communication," in *in Wireless Networks of Biosensors Implanted in the Human Body, Workshop on Wireless Security and Privacy (WiSPr), International Conference on Parallel Processing Workshops, 2003*, 2003.

[11] K. K. Venkatasubramanian and S. K. S. Gupta, "Security for pervasive health monitoring sensor applications," in *ICISIP '06: Proceedings of the 4th International Conference on Intelligent Sensing and Information Processing*, Bangalore, India, December 2006, pp. 197–202.

[12] F. M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: Resource-efficient key management and signal-level data scrambling," *EURASIP Journal on Advances in Signal Processing*, vol. vol. 2008, 2008.

[13] T. Falck, H. Baldus, J. Espina, and K. Klabunde, "Plug 'n play simplicity for wireless medical body sensors," *Mob. Netw. Appl.*, vol. 12, no. 2-3, pp. 143–153, 2007.

[14] G. Li, J. He, and Y. Fu, "A hexagon-based key predistribution scheme in sensor networks," in *ICPPW '06: Proceedings of the 2006 International Conference Workshops on Parallel Processing*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 175–180.

[15] S. A. Çamtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 15, no. 2, pp. 346–358, 2007.

[16] M. Eltoweissy, M. H. Heydari, L. Morales, and I. H. Sudborough, "Combinatorial optimization of group key management," *J. Netw. Syst. Manage.*, vol. 12, no. 1, pp. 33–50, 2004.

[17] G. Dini and I. M. Savino, "An efficient key revocation protocol for wireless sensor networks," in *WOWMOM '06: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 450–452.

[18] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[19] M. R., M. R., and E. M., "TKGS: Threshold-based key generation scheme for wireless ad hoc networks," in *IEEE International Conference on Computer Communication and Networking(ICCCN'04)*, October 2004.

[20] S. M. K. ur Rahman Raazi, H. Lee, S. Lee, and young Koo Lee, "MUQAMI+: a scalable and locally distributed key management scheme for clustered sensor networks," *Annals of Telecommunications*.