Secure & Energy Efficient key Management Scheme for WBAN – A Hybrid Approach

Iehab A. AL-Rassan[†], **Naveed Khan**[††]

[†,††]Department of computer Science, College of Computer & Information Sciences King Saud University Riyadh , Saudi Arabia

University of Maryland, College Park, MD, USA

Summary
Wireless body area network (WBAN) is a network of wireless sensor nodes, which monitor mobile health when placed carefully on the human body or in the wearable cloths. WBAN have a great potential for the growth and development of the future ubiquitous health systems, however; the security concern associated with the current WBAN is an alarming challenge. Security of a body area network (BAN) is unavoidable as it is mainly used for securing the life of patients and soldiers. By securing the BAN we actually secure the life of its wearer. Two techniques i.e. Physiological values (PV's) based key management ,which generate random keys by using the vital signs of human body and Pre-loading based scheme, which will be used to strengthen the security of our PVs based scheme. The potential limitation of PV's is short keys generation, which can be easily brute forced and high computational cost whereas in Pre-loading the keys are not random and require enough keys storage. In this paper we will merge PV's and pre-loading techniques by using electrocardiography (EKG/ECG) values of PVs and pre-loading based schemes to strengthen the security. The applied technique will enhance the security as well as reduce storage and power consumption.

Key words:
Physiological values (PV's), Electrocardiogram (EKG/ECG), Wireless body area network (WBAN)

1. Introduction

Sensor Network development comprised of sensor node for monitoring electric power and load, real time traffic building safety (structural fire and physical security), military sensing and tracking. However, human health monitoring has got tremendous focus of the researchers in health care where a complete technical revolution is expected. WBAN is increasingly becoming important recently due to the reliable data acquisition in the mobile state. WBAN is a network of motes distributed in different places in a small area. These most includes an integrated microprocessor, data acquisition system, radio, sensors, and a power source. These motes/devices sense, process and communicate data of physiological (heart beat, motion, respiration and body temperature, etc) and environmental conditions (temperature, sound, vibration or pressure) to the base station by sending message or start emergency alarm to inform the authority. Therefore WBAN finds potential applications in healthcare, environmental monitoring and home automation and disaster management [1, 2].

Figure 1 shows overall architecture of a WBAN. The physiological parameters consist of heartbeat, body temperature; motion etc. These parameters are measured and connected around the body by intercommunicating sensors(motes). All these features constitute WBAN. These sensors collect data from the body and send it to a base station for processing and storage, usually through a wireless multi-hop network [3,4]. Then base station sends the data to the medical server via internet (Figure 1). As BANs works on Physiological values which is sensitive information, so providing security to the inter-sensor communication within a BAN is much more important.

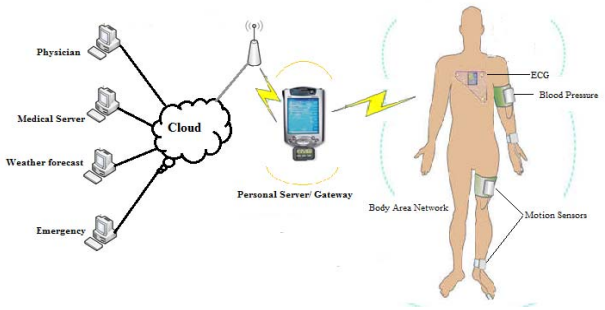

Figure 1 Architecture of a typical Wireless Body Area Network

BAN is an emerging technology, which is widely used for research in literature, military, healthcare, sports and first responder, etc [1, 2,3]. It consists of wearable intercommunicating sensors, as shown in Fig 1. The sensors are wirelessly connected onto human body for monitoring body movement and measuring physiological parameters such as body temperature, cardiac motion and so on [4] They collect data and send it to the base station through wireless multi-hop network [1] for analysis, storage and processing. The data are then sending in a

Manuscript received June 5, 2011
Manuscript revised June 20, 2011

secure manner to remote medical servers through internet or other communication media. Security is important because the data may contain sensitive information obtained from physiological values hence providing security to the inter-sensor communication which is more essential [5]. In fact, the requirement for protecting health data is legal as from the health insurance policy and accountability act (HIPAA) [6], which authorize that all individual personal information should be protected and safe from unauthorized access. The main purpose of BAN is to secure human life because it deals with human body and its physiological values to securely distribute cryptographic key in the BAN [7] which may enable us to handle emergency situation(specific event of heart attack) in correct time [8]. BAN's are widely used in various applications such as an intelligent fire, safety, rescue system, entertainment system, museum or city guide, heart rate and performance monitoring in sports and infant monitoring [5- 8].

The rest of paper is organized as follows: Section II provides the related work and Section III describe the proposed scheme. Section IV concludes the paper.

2. Related work

Security in BAN has played an important role in health monitoring systems. In this part, we will review and discuss the performance of some methods, which have been reported for the implementation of security techniques in BAN. The active research in BAN is the key management problem. L. Eschenauer and V. D. Gligor [9] has proposed a critical probability pre-distribution technique to establish the initial trust between the sensor nodes. Before implementing this technique, each sensor first selected randomly a set of key from a pool of keys to establish a pairwise key and then the sensors shared the common keys that they selected earlier. Chan at al [10] have studied a technique called q-composite key pre-distribution, which consented two sensors to establish a pairwise key only when they shared at least "q" common keys. Chan at al. also have widened a random pairwise keys scheme to avoid node capture attacks. Perrrig et al. [11] have proposed a security architecture known as Security protocols for sensor Networks (SPINS) comprised of Sensor Network Encryption protocols (SNEP) and a combination of Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol(TESLA) and Sub network Access protocol (SNAP). In this architecture, SNEP provided data confidentiality whereas the combination of TESLA and SANP provided authentication for broadcast data. The overall architecture was designed in such a way that each sensor node shared a secret key with the base station. Using Perrrig architecture two sensors cannot share secret key until the key shared with base station. The base station acts as a trusted third party between the sensors. Oliveira at al [12] has analysed random key pre-distribution technique using hierarchal mechanism based on cluster protocols for instance Low-Energy Adaptive Clustering Hierarchy (LEACH) [13]. Similarly, others [14-16] have studied the random key pre-distribution technique of homogenous nodes for acquiring a balance distribution of random keys to make security possible for every node. But the drawback of these techniques is the communication overhead and high storage media, which is not considered to be a good choice for sensor nodes with low power consumption and storage media. Traynor et al. [17] have demonstrated a probabilistic unbalanced distribution of keys throughout the networks, that leverages the existence of a small percentage for more capable sensor not only provide an equal level of security but also reduces the consequences of nodes compromise. K. Lu et all. [18] have analyzed a key management scheme for heterogeneous sensors in a sensor network. The advantages of this scheme are; (i) minimum storage requirement for key generation process and (ii) small number of generation keys instead of generating a large pool of random keys. For generation of key chain a keyed- hash function is used and then these chains were further used for the collection of a key pool. F Kausar et al. [19] have proposed a key management technique for heterogeneous sensor networks in which the key pool is assigned to H sensors where as one key of that key pool is assigned to L sensor, the end result of this technique is to limited storage consumption and full network connectivity. PV's vary from person to person which shows its uniqueness for every individual due to this fact it was introduced for security purpose. S. D. Bao et al. [20] have proposed a technique in which PV's were used for authentication of an entity. The basic of the Bao's technique function is to collect process and then transmit data. The transmitted data is sent through use a secure channel to other sensor for authentication or recognition. K. Ouchi et al. has [21] presented a module, which have a shape of a wearable wrist watch. This module consists of a LCD with a vibrator speaker. The first one is used to display messages whereas the later is used to activate alarm in case of emergency situation. The basic function of this unit was to measure the physiological data and then sent this data through Bluetooth technology to personal Digital Assistant (PDA), which identifies the patient general framework. In addition, this module not only displayed the detailed information of patient, gave timely instructions on daily health care but also managed the overall patient data. K. Venkatasubramanian et al. [1] have projected a technique known as EKG based key agreement scheme using Fast Fourier Transform (FFT). As the computational cost of FFT is extracted which is O(nlogn) as discussed by Yi-leh Wu et al [22]. (SHA-

256) is used for exchanging the block by simply hashing function. Aftab et al. [23] have demonstrated that on the sender side the key generation phase is exchanged before the blocks. The blocks were first hashed by using SHA-256 and then watermark was included for security in the hashed blocks by using the finger prints as a seed to the random machine. The random numbers generated by the random machine were used as the locations for the watermarks to be embedded on the sender side. The same process is used to remove the watermark from the blocks on the receiving side. On the receiving end the watermark and pure hashes of the blocks are removed by using the position generated by fingerprints seeded random machine.

3. Proposed Scheme

In this section we proposed a secure and energy efficient key management scheme. our approach primarily consists of three steps.

A. *Physiological (PV's) based Scheme*

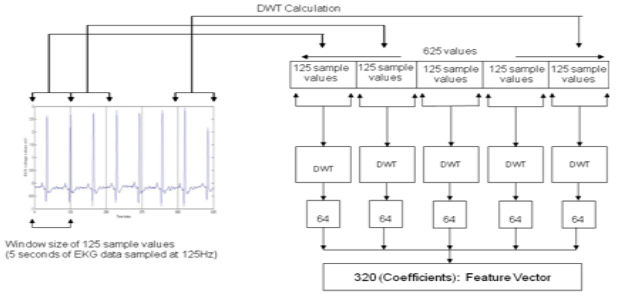

Figure 2: Feature Generation/Extraction using Discrete Wavelet Transform [23].

In this step energy efficient ECG based key management scheme will be proposed. We will collect PVs (ECG) from MIT physiobank [24]. After ECG collection the features will be extracted from the EKG values and then the key agreement phase will be used for the generation of pair wise keys. To secure inter-sensor communication features are extracted from EKG/ECG in BAN. For feature extraction discrete wavelet transform (DWT) will be used because of its flexible characteristics as its localized in both frequency and time domain and computationally inexpensive. The two sensors first samples the EKG/ECG signals at certain sample rate for specific time (125Hz sampling rate and 5 seconds duration) and filtered by removing unnecessary frequency components. The five seconds sample of the EKG signal (producing 625 samples) is then divided into 5 parts of 125 samples each. Discrete Wavelet Transform (DWT) is then applied on each part to extract features. The first 64 coefficients are selected from each part and form a feature vector of 320 values (see figure 2).

B. Pre loading based scheme

In this step a pre-loading based key management scheme will be proposed in combination with the PVs based scheme to strengthen the security of the overall architecture. In this scheme a key pool is established which have large number of keys loaded to H-Sensor and assume they are more powerful and consist of low end L-Sensor. Maximum keys are loaded to H-Sensor from a secure key pool and a single key to each L-Sensor node before deployment Pre-distribution [25].The key distribution network hierarchy will be as follows:

Key Pre-Distribution⇨Cluster Formation Phase ⇨Neighborhood Discovery Phase⇨Cluster head based shared Key Discovery Phase⇨ Addition of New Node.

This will strengthen the security of PV's based scheme as well as reduce storage and energy consumption.

We analyzed and evaluate the security of our technique in terms of Availability, Integrity and confidentially to strengthen our technique.

C. Analysis on the basis of Security, Energy and Storage Consumption.

As WBAN consists of low power sensors having limited power and storage capabilities, as the security mechanism should be lightweight both in terms of energy and storage. In this step we will analyze our proposed technique on the basis of energy and storage and we will also check the randomness and the uniqueness of the generated keys for the security of the technique.

The proposed approach will give new dimension to secure and energy efficient key management in wireless sensor network with lass power and storage consumption in the perspective of PV' based scheme and preloading based scheme .In our technique PV's of human will be used for generating random keys because of its time variant characteristics. The random key keys further used in pre-loading technique to strengthen the security and reduce power and storage consumption. Based on analysis and simulation the proposed strategies yields better result than existing ones.

4. Conclusion

In this paper, we proposed a secure and energy efficient key management scheme to secure inter sensor communication for Wireless Body Area Network. The basic idea is to use physiological values for generation of pair wise keys with randomness characteristics. By using these keys we are going to apply a pre-loading based scheme which pre-loads a small number of keys to H-sensors which could significantly reduce storage

requirement as well as consumes less energy. In addition it could also improve security for the sensors individual bases as well as for whole network.

References

[1] K.Venkatasubramanian, G. Deng, T. Mukherjee, J. Quintero, V. Annamalai, and S. K. S. Gupta. Ayushman.: A Wireless Sensor Network Based Health Monitoring Infrastructure and Testbed. In Distributed Computing in Sensor Systems, pages 406{407, July 2005.

[2] K. Hung and Y.T. Zhang. Implementation of a wapbased telemedicine system for patient monitoring. IEEE Transactions on Information Technology in Biomedicine,7(2):101–107, 2003.

[3] R.S.H. Istepanian, E. Jovanov, and Y.T. Zhang. Guest editorial introduction to the special section on m-health:Beyond seamless mobility and global wireless healthcare connectivity. IEEE Transactions on Information Technology in Biomedicine, 8(4):405–414, 2004.

[4] E. Jovanov, A. Milenkovic, C. Otto, and P.C. Groen. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. Journal of NeuroEngineering and Rehabilitation, 2005.

[5] Venkatasubramanian, A. Banerjee, and S. K. S. Gupta.: Plethysmogram-based Secure Inter-Sensor Communication in Body Area Networks. Pages 1–7, November 2008. In Proc. of IEEE Military Communications Conference.

[6] HIPAA-Report 2003, "Summary of HIPAA Health Insurance Probability and Accountability Act," US Department of Health and Human Service, May 2003.

[7] D. Singel, B. Latr, B. Braem, M. Peeters, M. D. Soete, P. D. Cleyn, B. Preneel, I. Moerman, and C. Blondia.: A secure cross-layer protocol for multi-hop wireless body area networks. In 7th International Conference on AD-HOC Networks and Wireless, September 2008.

[8] S. K. S. Gupta, T. Mukherjee, and K. Venkatasubramanian, "Criticality Aware Access Control Model for Pervasive Applications," March 2006,pp. 251–257, In Proc. of 4th IEEE Conference on Pervasive Computing Pervasive Computing and Communications.

[9] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks," in ACM CCS, 2002.

[10] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks," in IEEE Symposium on Security and Privacy, May 2003, pp. 197–213.

[11] A. Perrig, R. Szewczyk, J. Tygar, Victorwen, and D. E. Culler, "Spins: Security protocols for sensor networks," in Seventh Annual Int'l Conf. on Mobile Computing and Networks, July 2001.

[12] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro, "Sec leach: A random key distribution solution for securing clustered sensor networks," in 5th IEEE international symposium on network computing and applications, 2006, pp. 145–154.

[13] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energyefficient communication protocol for wireless microsensor networks," in IEEE Hawaii Int. Conf. on System Sciences, 2000, pp. 4–7.

[14] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networkss," in IEEE Symposium on Research in Security and Privacy, 2003.

[15] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach," in 11th IEEE International Conference on Network Protocols (ICNP'03), 2003.

[16] R. D. Pietro, L. V. Mancini, and A. Mei, "Random key assignment secure wireless sensor networks," in 1st ACM workshop on Security of Ad Hoc and Sensor Networks, 2003.

[17] P. Traynor, R. Kumar, H. B. Saad, G. Cao, and T. L. Porta, "Establishing pair-wise keys in heterogeneous sensor networks," in INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings, 2006, pp. 1–12.

[18] K. Lu, Y. Qian, and J. Hu, "A framework for distributed key management schemes in heterogeneous wireless sensor networks," in IEEE International Performance Computing and Communications Conference, 2006, pp. 513–519.

[19] F Kausar et al "Key Management and Secure Routing in Heterogeneous Networks"- IEEE International Conference on, 2008 - computer.org

[20] S. D. Bao, Y. T. Zhang, and Y.-T. Zhang:"Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems, September 2005, pp. 2455–2458, In Proc. of the IEEE 27th Conference on Engineering in Medicine and Biology.

[21] K. Ouchi, T. Suzuki, and M. Doi.: LifeMinder: " A Wearable Healthcare Support System Using User's Context," July 2002, pp. 791–792, In Proc. of 22th International Conference on Distributed Computing Systems Workshops.

[22] Yi-leh Wu , Divyakant Agrawal , Amr El Abbadi.:A Comparison of DFT and DWT Based Similarity Search in Time-Series Databases. In Proceedings of the 9th International Conference on Information and Knowledge Management. pages = {488--495} (2000).

[23] Aftab Ali and Farrukh Aslam Khan "An Improved EKG-Based Key Agreement Scheme for Body Area Networks" Communications in Computer and Information Science, 2010, Volume 76, 298- 308 DOI: 10.1007/978-3-642-13365-7_29.

[24] http://www.physionet.org/physiobank/database/mitdb/

[25] K. Lu, Y. Qian, and J. Hu. "A framework for distributed key management schemes in heterogeneous wireless sensor networks". In IEEE International Performance Computing and Communications Conference, pages 513–519, 2006.