A Novel Architecture for Efficient Key Management in Humanware Applications

Syed Muhammad Khaliq-ur-Rahman Raazi,
Sungyoung Lee, Young-Koo Lee

Ubiquitous Computing Laboratory, Department of Computer Engineering
Kyung Hee University (Global Campus)
Yongin-si, Korea
{raazi, sylee}@oslab.khu.ac.kr, yklee@khu.ac.kr

***Abstract*— In humanware applications, resource constrained sensor devices are tactically placed on human body to form Wireless Body Area Networks (WBAN). Then the WBAN is used for monitoring biometrics and movements of human body. Keeping in mind the resource constrained devices, WBANs are treated just like wireless sensor networks when considering a solution for key management. However, WBANs differ from traditional wireless sensor networks in scale, topology and security requirements. Also, the WBANs can also use random values from biometric measurements for the generation of keys. These differences render the key management schemes of WSNs inefficient and overly complex for WBANs scenario. Therefore, we propose a key management scheme that is efficient and fulfills the security requirements of WBAN.**

key management; humanware; body area networks; security; life care

I. INTRODUCTION

WBANs are small area networks that are designed to gather body related information from different parts of the human body. Nodes are placed at various parts of the body to measure biometrics through their sensors. All information is gathered at a central node and then sent to a server, which uses this information according to the application.

There are a number of applications for which WBAN are used. Most important applications of WBAN are in healthcare. Healthcare includes care for patients in hospitals or care centers and for patients, who are at their houses. Patients admitted in hospitals or care centers include the patients, who are unconscious, in coma or under intensive care. This care is important for many outpatients also e.g. care for elderly people and high risk pregnancies. These patients require timely and accurate medical care otherwise their lives may be at stake.

With the introduction of sensor devices forming WBAN on patients' body, patients' sensitive medical information can be relayed to the central server in real time. Based on the patients' medical information, customized software can generate alerts for the concerned medical staff, which can react in a timely manner. Emergency situations include heart attack or sudden increase in blood pressure of a woman going through high risk pregnancy. Apart from healthcare, WBAN also has its applications in studying athletes' bodies for certain reasons.

Security is an essential part of WBANs and key management plays pivotal role in ensuring security in any network. We have to make sure that patient's data is transferred to the central server correctly and confidentially i.e. unauthorized users are not allowed to access the patient's information. Also, we have to guard against spoofing and cryptanalytic attacks. In this paper, we have proposed a lightweight scheme for providing the required level of security in WBANs.

Rest of this paper is organized as follows: section 2 discusses the related work and outlines the problem statement. Section 3 presents models and assumptions. Proposed scheme is presented in section 4. Analysis of the proposed scheme and its comparison with other schemes is done in section 5. Paper is concluded in section 6.

II. RELATED WORK AND PROBLEM STATEMENT

Traditionally, WBANs have been treated just like any other Wireless Sensor Networks. Most of the related work falls under the wider umbrella of Wireless Sensor Networks. In this regard, much work has been done in this area. Most simple form of key management is key pre-distribution. In key pre-distribution schemes, keys are loaded in the sensor nodes prior to their deployment. Much research has been done in finding efficient ways of key distribution prior to node deployment [1][2][3][4]. In all key pre-distribution schemes, it is assumed that the networks are short-lived and will not require re-keying. This notion is not applicable in practical scenarios. Re-keying is necessary in order to avoid cryptanalytic attacks on sensor networks.

In order to avoid problems with static key management schemes, many dynamic key management schemes have been proposed [5][6][7][8][9][10]. These dynamic key management schemes also include provisions for re-keying and node revocation. All dynamic key management schemes have been designed keeping in mind the requirements of wireless sensor networks. Most of the research community has been inclined towards applying the solutions for wireless sensor networks in WBAN domain. However, it is not suitable to do so because WBANs are different from wireless sensor networks in many aspects.

Most importantly, these two networks differ in scalability. Wireless sensor networks are large scale networks while WBANs are small scale networks. Patients are likely not to wear more than a few sensor nodes. Secondly, in WBANs all nodes are in communication range of each other unlike wireless sensor networks. This is because the whole network is formed on the human body, which is not a very large area. This difference automatically takes care of attacks that involve routing.

Apart from the above two differences, a compromised node can easily be removed from the scene in WBAN while it can not be removed easily from the scene in wireless sensor networks. In some scenarios of WBAN, a compromised node must be replaced with another node. For example, if only one node is measuring a certain biometric such as heart rate, it must be replaced. Instead of revoking a compromised node through an algorithm, the compromised node can easily be removed from the scene or turned off by human intervention.

Another difference is that the nodes in WBANs are used to measure biometrics. Biometrics has been known to exhibit the properties of random numbers, which we can use as keys. Many researchers have used biometrics for key generation [11][12]. Also, some researchers argue that nodes in WBAN don't even need to exchange keys [13][14][15]. They argue that two nodes can sense the same biometric at one time and then apply error-correcting codes to get the same key at both nodes. However, there are many issues in such approaches like time synchronization. Also, we will need more sophisticated nodes so that they can monitor more than one biometric.

Due to the differences in scale, topology and security requirements of WBAN from wireless sensor networks, key management schemes for wireless sensor networks can not be applied to WBAN scenarios. To our knowledge, until now no one has proposed a key management scheme, which is specifically designed for WBANs.

III. System Model and Assumptions

In a typical WBANs scenario, there are a few sensor nodes worn by patients. They can all communicate with each other. Also, there is a Personal Server (PS) on each body. Job of PS is to gather all the bodily information and relay it to a medical server (MS), which resides in hospital or a healthcare center. MS can generate alerts based on the patients' information. Also, doctors and other concerned medical staff can access the patients' information from MS. Any internet enabled mobile device or PDA can be used as PS. Otherwise some sensor node can be elected or designated as a PS; it can relay information to the MS through a personal computer residing at home. System architecture assumed for WBAN in our scheme is shown in Fig. 1.

PS is also a resource constrained device just like other wearable sensor nodes because it also runs on a battery. We assume that unlike wireless sensor networks, adversary will not be able to capture a node physically. Adversary can passively eavesdrop or try to use an existing node's identity to send false information. All nodes are under human observation as it is typical in WBAN scenario.

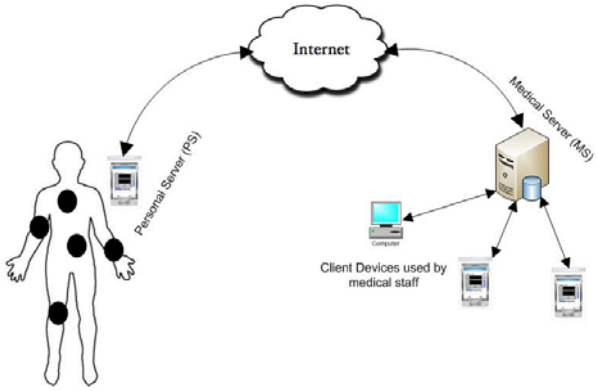

Figure 1. System architecture of wireless body area networks

IV. Proposed Scheme

In order to qualify as a key generating node, a node must have required strength in terms of energy, computation power or both. In other cases, nodes must have some other way to get true random numbers. In humanware applications, sensor nodes are used to sense and then measure biometrics from human body. Research has shown that values of biometrics sensed and then measured from human body are sufficiently random and these values can be used as key for encryption and other security purposes [11][12].

In our scheme, biometric measurements are used as symmetric keys because they exhibit the required properties of random numbers. All sensor nodes in the network have a separate basic key K_{bsc}, which is shared with the MS and is not known to any other node. This key is used very rarely and refreshed after every use. Since all nodes are in direct communication range of the PS, all sensor nodes share a pair-wise key K_{pw} with the PS. Also, there is another key K_{comm} shared throughout the network. K_{comm} is used for communication purposes. Since K_{comm} is used frequently, it might come under cryptanalytic attacks. Therefore, we use the pair-wise key K_{pw} to update K_{comm}. Since K_{pw} will be used less frequently, it will be relatively safe from cryptanalytic attacks. In the remaining part of this section, we will discuss the procedures for initial deployment, re-keying and node addition one by one.

A. *Initial Deployment*

Before deployment, the PS is pre-loaded with the initial value of K_{comm} and K_{pw} of all the nodes. PS is deployed first and then rest of the nodes join the network created by the PS. Initial deployment in done in the following way: -

1. Personal Server, preloaded with K_{comm} and K_{pw} of all the nodes, is deployed initially. After deployment, the PS establishes connection with the MS directly or through the internet.
2. In the second step, sensor nodes are deployed. Sensor nodes are pre-loaded with their basic key K_{bsc} and pair-wise key K_{pw}. As soon as it is deployed, each sensor node *i* sends a discovery

message to the PS. This discovery message is protected using K_{pw}^{i}.

3. PS sends communication key K_{comm} to each node i using its pair-wise key K_{pw}^{i}.

For re-keying purposes, the PS can use the chosen random values from biometric measurements, forwarded to it by the sensor nodes.

B. Re-keying

All keys must be refreshed in a timely manner in order to avoid cryptanalytic attacks. Communication key is refreshed in the same way as it is first distributed. In order to refresh the communication key, the PS does not have to generate a key. It just needs to randomly select a value from already existing biometric measurements that the sensor nodes forward to it. Whenever re-keying is required, the PS server just sends the new value of K_{comm} to every node individually using their pair-wise keys K_{pw}^{i}.

On the other hand, pair-wise key K_{pw} is refreshed by sensor nodes rather than the PS. In order to refresh its K_{pw}^{i}, sensor node *i* uses a random value from among the biometric measurements it records. It uses this random value as new value of pair-wise key K_{pw}^{i} and sends it to the PS using the previous value K_{pw}^{i}.

All keys are refreshed after specific time intervals. However, if PS wants to refresh a key at some other time instant, it can request the specific node *i* to send a new key value in case key K_{pw}^{i} need to be refreshed. Sensor node $_{i}$ sends key refreshment message immediately after it receives instructions from the PS. For K_{comm}, the PS just sends key refreshment message itself.

If K_{pw}^{i} of a sensor node *i* is compromised, it is refreshed using its basic key K_{bsc}^{i} in the following manner: -

1. PS informs the Medical Server (MS) that K_{pw}^{i} is compromised.
2. MS generates a new value of K_{pw}^{i} and sends it to the PS.
3. MS generates a new value of K_{bsc}^{i}. MS encrypts the new value of K_{pw}^{i} and K_{bsc}^{i} in the current value of K_{bsc}^{i} and sends it to the PS.
4. PS forwards the new values of K_{pw}^{i} and K_{bsc}^{i} to the sensor node *i*.

The network functions normally after this point in time. Note that the PS never comes to know the value of K_{bcs}^{i}. This is important if we want to secure the network in case the PS is compromised.

C. Node Addition

Node addition takes place in a similar way as the initial deployment with the help of following steps: -

1. MS informs the PS about new nodes and sends their pair-wise key K_{pw}^{i} to the PS.
2. New nodes, pre-loaded with their respective K_{bsc}^{i} and K_{pw}^{i} are deployed in the network.
3. New nodes send their discovery messages to the PS using their respective K_{pw}^{i}.
4. PS sends the current value of communication key K_{comm} to new nodes using their respective pair-wise keys K_{pw}^{i}.

Normal functions in a normal way after this point in time. All communications between the PS and the MS use a secured internet connection in order to maintain privacy of individuals. Similarly, the initial value of pair-wise key K_{pw}^{i} of a new sensor node *i* is transferred to the PS through the internet using a secured connection between the PS and the MS.

V. ANALYSIS AND COMPARISON

In this section, we will analyze our scheme's communication and computation overheads and then compare them with the overheads of two existing state-of-the-art schemes LEAP+[7] and MUQAMI[10].

In the initial deployment phase of our scheme, all nodes are pre-loaded with the initial values of K_{pw}. All nodes send initial discovery message to the PS using their respective K_{pw} and then they are sent K_{comm} one by one. If the total number of nodes in a WBAN, excluding the PS, is *n*, then the total number of messages exchanged in the initial deployment phase of our scheme can be expressed as

$$MSG\_COUNT^{INIT} = 2n \quad (0.1)$$

In case of the key refreshment phase, every node has to send to the PS one message each. So, the communication overhead of our scheme in key refreshment phase, in terms of the number of messages exchanged, can be expressed as

$$MSG\_COUNT^{REKEY} = n \quad (0.2)$$

Comparison of our scheme with the other two schemes is presented in Table 1. Our scheme proves to be better than the other two schemes just because we have designed our scheme keeping in mind the requirements of WBANs rather than the requirements of wireless sensor networks as is the case in other schemes.

Fig. 2 compares the communication overhead of our scheme with other schemes in the initial deployment phase. Similarly, Fig. 3 compares the communication overhead of the re-keying phase. Our scheme performs better than the two other schemes in both phases.

TABLE I. COMPARISON OF THE THREE SCHEMES WITH RESPECT TO COMMUNICATION AND COMPUTATION OVERHEAD

Scheme		Proposed Scheme	LEAP+	MUQAMI
Comm. Overhead	Initial Deployment	2n	(n+1) ×(2n+1) +1	2n+n
Comm. Overhead	Re-keying	n	(n+1)×n	2n
Comp. Overhead	Initial Deployment	1	(n+1) ×(2n+1)+ 1	n+1

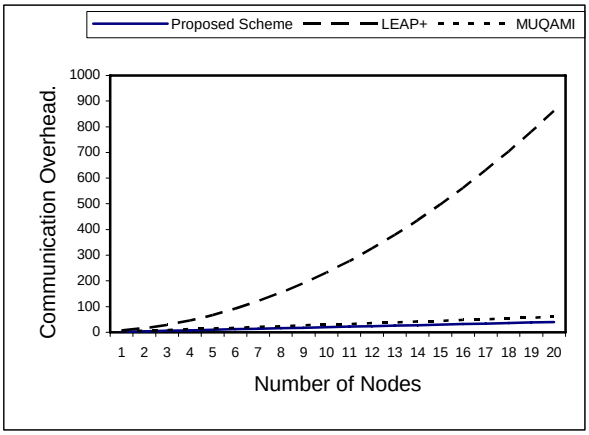

Figure 2. Comparison of our scheme with the other two schemes considering the initial deployment phase

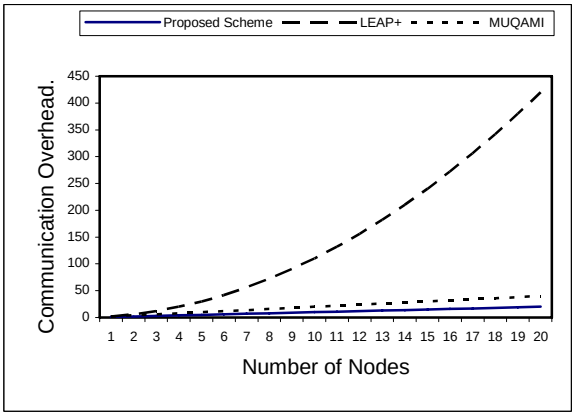

Figure 3. Comparison of our scheme with the other two schemes considering the re-keying phase

The two graphs look similar but if we have a closer look, our scheme is even more efficient in the re-keying phase (note the difference between our scheme and MUQAMI in the both phases). It is always desirable to have more efficiency in the re-keying phase rather than the initial deployment phase because re-keying is a recurring phase and the initial deployment takes place only once.

Apart from the communication overhead, we also need to consider the computation overhead. Our scheme does not have any computation overhead in re-keying phase because all the keys are generated using biometrics. We assume that other schemes also use biometrics for re-keying. However, our scheme performs a lot better in the initial deployment phase because it requires only the PS to generate one key K_{comm}. Other schemes have to generate more keys as compared to our scheme. In the following, we analyze the number of keys other schemes have to generate during the initial deployment phase.

In case of LEAP+, every node has to verify all other nodes (as all nodes are in communication range of each other). Also, it has to compute pair-wise keys with all nodes. In addition to that, every node generates its cluster key, which makes the total number of computations equal to $2n+1$. Since there are $n+1$ nodes in the network, this factor will be multiplied to get the total number of computations in the initial deployment phase of LEAP+. Finally, the PS has to generate the communication key also. So, the total number of computations required in the initial deployment phase of LEAP+ can be expressed as

$$COMP\_COUNT^{INIT}_{LEAP+} = (n+1)\times(2n+1)+1 \quad (0.3)$$

Similarly, about n keys are generated by the PS in case of MUQAMI so the nodes can communicate with each other. If we also add the one communication key it generates in the initial deployment phase, computation requirements of MUQAMI come out to be

$$COMP\_COUNT^{INIT}_{MUQAMI} = n+1 \quad (0.4)$$

Table 1 also compares the computation overhead of the three schemes in the initial deployment phase.

VI. Conclusion and Future Work

In this paper, we have presented a key management scheme that was designed specifically keeping in mind the requirements of wireless body area networks. We have established that the requirements of wireless body area networks differ from the requirements of wireless sensor networks in many different ways. Therefore, the application of key management schemes used for wireless sensor networks in WBAN paradigm is not a feasible solution.

This paper primarily focuses on the protection against attacks in terms of confidentiality, integrity and authenticity. However, these do not address all the concerns in security. Protection against attacks, which compromise availability, is another important aspect of security. Also, attack prevention is better than attack mitigation. These other concerns constitute the future work and the future direction of this research.

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)).

References

[1] Li, G., He, J., Fu, Y.: A hexagon-based key predistribution scheme in sensor networks. In: ICPPW '06: Proceedings of the 2006 International Conference Workshops in Parallel Processing, pp. 175-180. IEEE Computer Society, Washington, DC, USA (2006). DOI http://dx.doi.org/10.1109/ICPPW.2006.9.

[2] Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy, p. 197. IEEE Computer Society, Washington, DC, USA (2003).

[3] Du, W., Deng, J., Han, Y.S., Varshney, P.K.: A pairwise key pre-distribution scheme for wireless sensor networks. In: CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, pp. 42-51. ACM, New York, NY, USA (2003). DOI http://doi.acm.org/10.1145/948109.948118.

[4] Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. In: CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, pp. 41-47. ACM, New York, NY, USA (2002). DOI http://doi.acm.org/10.1145/586110.586117.

[5] Shaikh, R., Lee, S., Khan, M., Song, Y.: LSec: Lightweight security protocol for distributed wireless sensor networks. In: 11th IFIP International Conference on Personal Wireless Communications PWC'06, LNCS, vol. 4217, pp. 367-377. Spain (2006).

[6] Dini, G., Savino, I.M.: 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, pp. 450-452. IEEE Computer Society,Washington, DC, USA (2006). DOI http://dx.doi.org/10.1109/WOWMOM.2006.23.

[7] Zhu, S., Setia, S., Jajodia, S.: LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Trans. Sen. Netw. 2(4), 500-528 (2006). DOI http://doi.acm.org/10.1145/1218556.1218559.

[8] Ghumman, K.: Location-aware combinatorial key management scheme for clustered sensor networks. IEEE Trans. Parallel Distrib. Syst. 17(8), 865-882 (2006). DOI http://dx.doi.org/10.1109/TPDS.2006.106. Senior Member-Mohamed F. Younis and Senior Member-Mohamed Eltoweissy.

[9] Paek, K.J., Kim, J., Hwang, C.S., Song, U.S.: An energy-effcient key management protocol for large-scale wireless sensor networks. In: MUE '07: Proceedings of the 2007 International Conference on Multimedia and Ubiquitous Engineering, pp. 201-206. IEEE Computer Society, Washington, DC, USA (2007). DOI http://dx.doi.org/10.1109/MUE.2007.74.

[10] Raazi, S.M.K., Khan, A. M., Khan, F.I., Lee, S.Y., Song, Y.J.: MUQAMI: A Locally Distributed Key Management Scheme for Clustered Sensor Networks. In: IFIPTM 2007: Proceedings of the 2007 Joint iTrust and PST conferences on privacy, trust management and security, Moncton, New Brunswick, Canada. 30 July - 2 August 2007 pp. 333-348.

[11] Poon, C.C.Y., Zhang, Y.T., Bao, S.D.: A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Communication Magazine 44(4), 73-81 (2006).

[12] Cherukuri, S., Venkatasubramanian, K.K., Gupta, S. K. S.: BioSec: A Biometric based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body. Proceedings of the IEEE Int'l. Conf. Parallel Processing Workshop., 6–9 Oct. 2003, pp. 432–39.

[13] Venkatasubramanian, K. K., Gupta, S. K. S.: Security for Pervasive Health Monitoring Sensor Applications. In: ICISIP '06: Proceedings of the 4th International Conference on Intelligent Sensing and Information Processing, pp. 197–202, Bangalore, India, December 2006.

[14] Bui, F.M.,Hatzinakos, D.: 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 Volume 2008 (2008), Article ID 529879, 16 pages doi:10.1155/2008/529879.

[15] Falck, T., Baldus, H., Espina, J., Klabunde, K.: Plug 'n Play Simplicity for Wireless Medical Body Sensors. Journal of Mobile Networks and Applications (Springer Netherlands) 12(2-3), 143-153 (2007). DOI 10.1007/s11036-007-0016-2.