Channel Information based Cryptography and Authentication in Wireless Body Area Networks

Zhaoyang Zhang
University of Massachusetts Dartmouth
285 Old Westport Road
North Dartmouth, MA 02747
zzhang1@umassd.edu

Honggang Wang
University of Massachusetts Dartmouth
285 Old Westport Road
North Dartmouth, MA 02747
hwang1@umassd.edu

Athanasios V. Vasilakos
University of Western Macedonia
GR 50100 Kozani, Greece
vasilako@ath.forthnet.gr

Hua Fang
University of Massachusetts Medical School
Worcester, MA 01655
Hua.Fang@umassmed.edu

ABSTRACT

Wireless Body Area Networks (WBANs) are the core of components of future m-Health system and is playing a crucial role in healthcare applications. A key requirement for such applications is secure communications between body sensors. This paper presents a novel key agreement scheme which allows wireless body sensors in WBANs to share a common key generated using wireless channel information. Unlike traditional biometric based security approach, the proposed key agreement does not need extra hardware, which can secure data communications in a plug-n-play manner. Our experimental results show that the proposed scheme is feasible for WBANs.

Categories and Subject Descriptors

G.4 [**Mathematics of Computing**]: Mathematical Software; K.6.5 [**Management of Computing and Information System**]: Security and Protection—*Authentication*

General Terms

Security, Algorithms, Verification

Keywords

Wireless Body Area Networks (WBANs), Authentication, Wireless Channel, Security

1. INTRODUCTION

Wireless Body Area Networks (WBANs) are becoming more and more critical with the aged tendency of global populations. Many researchers focus on the application development of WBANs that can provide healthcare services to individuals. In general, a WBAN system consists of implanted or on-body medical sensor and contextual sensors. These sensors are able to measure body vital signs and motions in a real-time manner and can forward the data to remote servers for further processing.

Security is one of major concerns for WBAN applications. When a sensor in a WBAN system sends out a message, only the sensors on the same human body should be able to decrypt the received message. One possible solution is to pre-distribute keys before the deployment of a WBAN system. However, the approach needs human intervention when adding new sensors or replacing current sensors. Compared with a dynamic key approach, the static key is more vulnerable to the attackers. In order to overcome the limitations of the pre-distribution key method, some researchers have proposed to use biometric information of human body to secure the wireless communications among body sensors. This approach does not need pre-distributed key, thus it can work in a plug-n-play manner. Also, the key is randomly generated and time-varying. It is hard for attackers to attack the key if they do not have the same biometric information. However, the biometric method needs extra hardware that can collect biometrics.

In this paper, we propose a novel cryptography and authentication scheme which allows body sensors to share a common key generated from the wireless channel between them. The received signal strength indicator (RSSI) values are sampled and channel feature sets are generated. The channel feature set are used as keys to secure data communications over wireless channels by using Improved Juels and Sudan (IJS) algorithm.

The rest of this paper is organized as follows. Section II describes the related works. Section III briefly introduces wireless channel property and the Improved Juels and Sudan (IJS) algorithm. Section IV illustrates the system model of the proposed channel based cryptography and authentication scheme. Section V shows experiment and performance analysis. In Section VI, we conclude the paper, and discuss some possible future directions.

BODYNETS 2013, September 30-October 02, Boston, United States

DOI 10.4108/icst.bodynets.2013.253689

2. RELATED WORK

One solution to support secure communication is using key pre-distribution [4]. However, this method need human intervention and it is inconvenient when adding new sensors or replacing current ones. Using biometric information to secure the wireless communication is promising for WBAN applications. It does not need key pre-distribution and uses dynamic keys. The authors in [9, 10, 12] proposed to use ECG/EKG as a seed to generate a random key which is used to secure the wireless channel. However, the method in [9] needs extra hardware to collect biometric information and has a significant communication overhead. The method in [12] also needs extra hardware though it uses a Improved Juels and Sudan algorithm to reduce the communication overheads.

Recently, researchers are studying the feasibility of using the wireless channel information to secure the communication [5, 8, 1, 11, 6]. The authors in [5, 1, 11] proposed to using channel information to secure the communication between body sensor and external users. In [8, 6], the authors proposed to using channel information to distinguish on body and off body sensors. Unlike them, In this paper, we propose a channel based cryptography and authentication scheme for WBAN applications based on IJS algorithm, which can significantly reduce the communication overheads. Its significant advantage is that no extra hardware is required. We also propose a feature generation methods that deal with slow channel variation.

3. PRELIMINARY

3.1 Wireless Channel

In this paper, wireless channel information is used to secure data transmission.

Two sensors in a WBAN, A and B, are able to communicate with each other, the signal sensor A received from sensor B and sensor B received from sensor A are presented as follows:

$$Y_A = h_{BA}X_B + n_A \quad (1)$$

$$Y_B = h_{AB}X_A + n_B \quad (2)$$

respectively, in which Y_A and Y_B are the signal received at sensor A and sensor B; $h_{AB} \approx h_{BA}$ are the channel gain between sensor A and sensor B; X_A and X_B are the signals from sensor A and sensor B; n_A and n_B are the Gaussian noises with variance σ^2. Because only one sensor is transmitting at a time, so if there is a Eve, the signal it can receive is

$$Y_E = \begin{cases} h_{AE}X_A + n_E & \text{if A is transmitting} \\ h_{BE}X_B + n'_E & \text{if B is transmitting} \end{cases} \quad (3)$$

According to the channel reciprocity, $h_{AB} \neq h_{AE}$ and $h_{BA} \neq h_{BE}$, thus in the low noise environment, if the transmission power levels of sensors A and B are the same and the RSSIs at both sensor A and B are mostly identical, the RSSIs can be used as keys to secure the wireless communication.

3.2 Fuzzy Vault and IJS Algorithm

The Fuzzy Vault algorithm proposed in [3] locks a secret in a vault using a set of values $F = \{f_1, f_2, \ldots, f_n\}$. The vault can be unlocked only with another set of values $F' = \{f'_1, f'_2, \ldots, f'_n\}$ which has a significant number of common elements with set F. In the fuzzy vault scheme, the Chaff points can not be chosen at random. If $y_i = p(x_i)$ for some chaff points, the security of the vault is reduced. To solve this problem, Y. Dodis et al. proposed an Improved Juels and Sudan algorithm (IJS) [7]. In IJS algorithm, the sender construct a unique monic polynomial using F as roots and sends a part of the coefficients to the receiver. The receiver can reconstruct the polynomial only when it has a set F' that shares significant common elements with F.

Lock:

1. Constructing a n-th order monic polynomial $p(x) = 0$ for all $x \in F$.
2. Sending coefficients of $p(x)$ from degree $n-1$ to $n-t$.

Unlock:

1. Constructing a polynomial $p_h(x)$ using the received t coefficients.
2. Evaluating p_h over F' to get $(f'_i, p_h(f'_i))$.
3. Searching for a polynomial $p_l(x)$ using Reed-Solomon decoding.
4. Reconstruct the polynomial by $p(x) = p_h(x) - p_l(x)$ if the above searching successes.

Consider the following example that illustrates the process of the IJS. Let set $t = 1$, $F = \{1, 3, 4\}$ and set $F' = \{1, 3, 5\}$, then $p(x) = \prod(x - f_i) = x^3 - 8x^2 + 19x - 12$. The information sending from the sender to the receiver is -8. The receiver first constructs $p_h = x^3 - 8x^2$, and then evaluates f_h over F' to get $(1, -7), (3, -45), (5, -75)$. After Reed-Solomon decoding, it gets $p_l = -19x + 12$ and finally reconstructs the polynomial by $p(x) = p_h(x) - p_l(x) = x^3 - 8x^2 + 19x - 12$.

Compared with the original Fuzzy Vault Scheme, the IJS algorithm does not use the Chaff points to secure the information. The advantages of the IJS algorithm over the Fuzzy Vault scheme are: (i) it avoids an insecure problem introduced by "non-random" Chaff points;(ii) it reduces the transmission overheads caused by Chaff points; (iii) it reduces complexity of searching process from nth-order polynomial to $(n-t)$th-order, which results in faster responding and lower energy consumption.

4. SYSTEM DESIGN

A WBAN system contains a set of physiological and environmental monitoring sensor nodes. These sensors are able to collect body vital signs and contextual information at a certain interval and send them to a highly capable device via a multi-hop network for further processing [2]. In this paper, we assume that all sensors in a WBAN can send data through wireless channel. We have proposed to use wireless channel information to secure the sensing data. The proposed method has the following advantages: (i) it does not need extra hardware and (ii) it does not need key distribution. Thus the proposed method can work on small sensors in a plug-n-play manner.

In the proposed channel information based typography and authentication scheme, both the sender and receiver measure the RSSI and generate feature sets. Then the channel

features F and F' are extracted from the sender (sensor A) and the receiver (sensor B), respectively. At the sender, the channel features form a secret k, which will be used to encrypt the messages (body vital signs) that need to be transmitted with data or general message. After the locking process of the IJS algorithm, t coefficients of the monic polynomial are sent to the receiver, along with the encrypted message and the Hash value based Message Authentication Code (MAC).

At the receiver, after the receiver gets the packet, it could recover the secret using the channel features F' it measured after the unlocking process of the IJS algorithm. Then it decrypts the encrypted message and calculates the MAC code using the same Hash function. The results will be compared with the received MAC to complete the authentication precess. The whole process is described in Fig. 1.

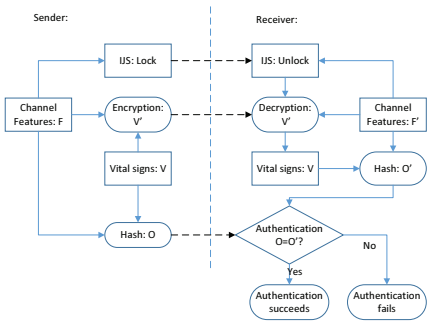

Figure 1: Channel Information based cryptography and authentication

4.1 Key Generation

In this paper we consider the secure communication between two sensors (sensor A and sensor B) in a WBAN system. The first process of the proposed method is to generate secure keys from the RSSI values. The process of sampling the RSSI is as follows:

1. The sensor A initiates the sampling process by transmitting packets with sequential counter values.
2. The sensor B records the RSSI values and responds to each with a ACK packet containing the same counter values and the RSSI.
3. The sensor A receives the ACK messages and records the RSSI for each transmission.

In the sampling process, the paired transmission should be close together in order to track channel variation in both directions simultaneously. The RSSI values are recorded and indexed as per probe counter value. The sampling process will stop when the there are enough RSSIs to generate a feature set.

When the sampling process stops, we generate feature set from the RSSI values: (i) For both sensor A and sensor B, put the RSSI values in a time order. (ii) Draw a curve containing all the values and find all inflection points. (iii) Each of these inflection point index and value are quantized and converted into a binary string and concatenated to form a feature. (iv) The features forms a feature set. After the above process, sensor A and sensor B will have a feature set $F = f_1, f_2, \ldots, f_n$ and $F' = f'_1, f'_2, \ldots, f'_n$, respectively. By choosing the index and value of a inflection point as a feature, we take the advantages of the temporal variations of the channel and ensure the security of the communication, especially when the two sensors are under a static condition. However, under the static conditions, the sampling will take longer time.

4.2 Cryptography and Authentication

Suppose that sensor A wants to send a message V to sensor B wirelessly. Firstly, two sensors initiate the sampling to generate the feature set F and F'. Then the feature sets are used as a secret key to ensure the security of the wireless communication. The process of cryptography and authentication is as follows:

Encryption:

1. At sensor A, the feature set F is used as a secret key to encrypt the message V, $V' = Enc(V, F)$.
2. The feature set F is used to construct a monic polynomial by IJS algorithm.
3. Generate a MAC value using a Hash function for F and V, $O = MAC(F|V|N_0)$.
4. Send out a message containing the IDs of the sensor, t polynomial coefficients, encrypted message and the hash value, $\{ID_A, ID_B, V', N_0, O\}$.

Decryption and Authentication:

1. Sensor B reconstruct the polynomial by F' and the t coefficients and get the feature set F.
2. The feature set F is used as to decrypt the message V, $V = Dec(V', F)$.
3. Generate a MAC value using the same Hash function based on F and V, $O' = MAC(F|V|N_0)$.
4. Authenticate the sender and the message by comparing O and O'. If $O = O'$, the authentication succeeds, otherwise the authentication fails.

Here, ID_A and ID_B are the IDs of the sender and receiver, respectively. V represents a message that needs to be sent out, V' denotes the encrypted message of V. The encryption methods could be any standard encryption methods, such as RSA and DES. N_0 is random number against reply attacks. The Hash function used in this paper is Secure Hash Algorithm 1 (HMAC-SHA1) [9].

5. EXPERIMENTS AND RESULTS ANALYSIS

We conducted experiments to investigate the performance of the proposed channel information based cryptography and authentication methods. In our experiments, we used MicaZ motes, which runs TinyOS, operates in in the 2.4GHz, and were deployed on human body. One mote (sensor A) is strapped on an individual's right arm and the other mote (sensor B) is on the waist of the same person.

5.1 Results

We have studied the performance of the proposed method for two scenarios: resting and walking. In the resting instance, the carrier is sitting on a chair, while in the Walking instance, the subject is walking randomly. We also put several Eve sensor in the room to study the authentication and security performance of the proposed algorithm.

Figure 2 shows the RSSI measured at the sender, receiver and an eavesdropper for resting. In the first instance, the carrier was sitting on a chair with little movement. We can find that the RSSI are changing with time although the carrier does not move. When the carrier is walking, the RSSI are changes more frequently than sitting in our experiment.

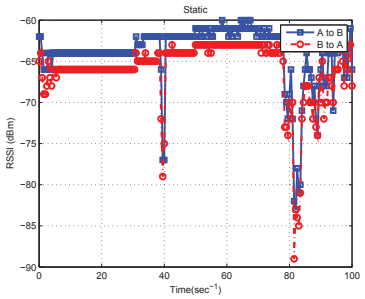

Figure 2: Resting

Figure 3 shows the FAR (False Acceptance Rate) performance respectively for different polynomial degree s and different tolerance t. As shown in Figure 3, it is observed that for the same t, the FAR decreases when the number of secure features s increases, and for the same s, the FAR increases when the number of helper information t is bigger.

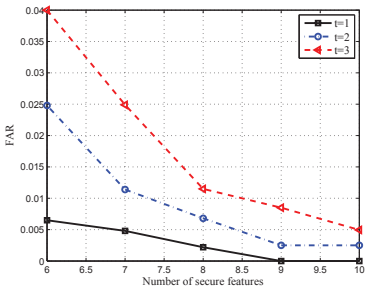

Figure 3: FAR versus number of secure features

6. CONCLUSION

In this paper, we developed a method that secures communications between body sensors in a WBAN system to protect data security and individual's privacy. We presented a novel key agreement scheme which allows body sensor in a WBAN system to share a common key generated from the wireless channel between them. The proposed algorithm does not need key pre-distribution and extra hardware. It uses a dynamic key and works in a plug-n-play manner. The experimental results show that the proposed scheme is feasible to secure wireless communications in a WBAN.

7. REFERENCES

[1] S. T. Ali, V. Sivaraman, and D. Ostry. Secret key generation rate vs. reconciliation cost using wireless channel characteristics in body area networks. *2010 IEEEIFIP International Conference on Embedded and Ubiquitous Computing*, pages 644–650, 2010.

[2] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung. Body area networks: A survey. *Mob. Netw. Appl.*, 16(2):171–193, apr 2011.

[3] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 523–540. Springer Berlin / Heidelberg, 2004.

[4] W. Drira, E. Renault, and D. Zeghlache. A hybrid authentication and key establishment scheme for wban. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 78–83, 2012.

[5] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen. Securing communications between external users and wireless body area networks. In *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy*, HotWiSec '13, pages 31–36, New York, NY, USA, 2013. ACM.

[6] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of the 15th annual international conference on Mobile computing and networking*, MobiCom '09, pages 321–332, New York, NY, USA, 2009. ACM.

[7] A. Juels and M. Sudan. A fuzzy vault scheme. page 408, 2002.

[8] L. Shi, M. Li, S. Yu, and J. Yuan. Bana: body area network authentication exploiting channel characteristics. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, WISEC '12, pages 27–38, New York, NY, USA, 2012. ACM.

[9] K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta. Pska: Usable and secure key agreement scheme for body area networks. *Information Technology in Biomedicine, IEEE Transactions on*, 14(1):60–68, 2010.

[10] H. Wang, H. Fang, L. Xing, and M. Chen. An integrated biometric-based security framework using wavelet-domain hmm in wireless body area networks (wban). *2011 IEEE International Conference on Communications ICC*, pages 1–5, 2011.

[11] H. Xiang and A. Yener. The role of channel states in secret key generation. *IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications PIMRC 2010*, pages 2679–2684, 2010.

[12] Z. Zhang, H. Wang, A. Vasilakos, and H. Fang. Ecg-cryptography and authentication in body area networks. *IEEE Transactions on Information Technology in Biomedicine*, 16(6):1070–1078, 2012.