Secure and Capable of Data Communication Procedure for Wireless Area Network

Supriya[1],Arun Kumar.H[2]

[1] Assistant Professor , Dept. of CSE , Rajiv Gandhi Institute of Technology, Karnataka, India

[2] Assistant Professor , Dept. of MECH , REVA Institute of Technology ,Karnataka, India

ABSTRACT

Wireless Body Area Networks (WBANs) are expected to play a major role in the field of patient-health monitoring in the near future, which gains tremendous attention amongst researchers in recent years. One of the challenges is to establish a secure communication architecture between sensors and users, whilst addressing the prevalent security and privacy concerns. In this paper,we propose a communication architecture for BANs, and design a scheme to secure the data communications between implanted/wearable sensors and the data sink/data consumers (doctors or nurse) by employing Ciphertext-Policy Attribute Based Encryption(CP ABE) and signature to store the data in ciphertext format at the data sink, hence ensuring data security. Our scheme achieves role-based access control by employing an access control tree defined by the attributes of the data. We also design two protocols to securely retrieve the sensitive data from a BAN and instruct the sensors in a BAN. We analyze the proposed scheme, and argue that it provides message authenticity and collusion resistance, and is efficient and feasible. We also evaluate its performance in terms of energy consumption and communication/computation overhead.

Keyword: -*Wireless Body Area Networks, Access Control; Secure Communications; Attribute-based Cryptosystem; Signature.*

1.INTRODUCTION

In recent years, innovative health-oriented networking and wireless communication technologies have been developed, which become an intrinsic part of many modern medical devices. The implantable medical devices (IMDs) [3], including pacemakers, cardiac defibrillators, insulin pumps, neuron stimulators, etc., utilize their wireless radios to deliver timely patient information, leading to a better health care monitoring system. Current advances make it possible to deploy battery-powered miniaturized IMDs on, in, or around the human body for long-term healthcare monitoring [4]. IMDs report their data to a data sink by wireless communication channels. The data sink can be an IMD designed to store data or a smartphone, which has the ability to communicate with a remote healthcare agency through cellular networks or the Internet. All those IMDs, which will later be simply referred as sensors, and the data sink together consist a small-scale wireless sensor network, called a Wireless Body Area Network (WBAN). WBAN as a key enabling technique for E-healthcare systems makes real-time health-related information accessible to medical specialists, who are then enabled to cast appropriate and timely medical treatment to the patients. The soaring national health expenditures and escalating age-related disabilities are shifting the emphasis from the hospital to the home [5], which makes WBANs a perfect candidate for enabling in-home monitoring and diagnosis, especially for people having chronic diseases. Unlike conventional sensor networks, a WBAN deals with more sensitive and important patient information that has significant security, privacy, and safety concerns, which may prevent the wide adoption of this technology [6]. As a sensor that collects patient information, all it cares is to distribute the information to authorized doctors and other experts securely. However, there are challenges everywhere: Data should be transmitted in a secure channel, and we all know the challenges in securing wireless communication channels. Node authentication is the most fundamental step towards a BAN’s initial trust establishment, key generation, and subsequent secure communications. There exist research that enables embedded sensors to establish a session key with each other by leverage physiological signals such as Electrocardiograph (ECG) [7], [8], [9], [10], [11], [12], [13]. Also, we can pre-distribute keys or secrets in sensors if necessary. From the perspective of cryptography, the high computation cost of asymmetric cryptography leaves symmetric encryption as the only viable option. But the key-distribution in symmetric encryption is challenging. And symmetric encryption is not a good choice for broadcasting a message because it involves some challenging issues, such as key-management and access control. At the same time, due to the limitation of memory space in sensors, a data sink, which has considerably larger memory and computation power, is employed to store data. To ensure the security of the data, we need to have certain level of protection to the data sink. However, a smartphone like device serving as the data sink can be physically lost or stolen, and an attacker can read the data once he captures the device. Moreover, recent research disclosed that smartphones suffer from severe privacy concerns since many applications often cross the line and read sensitive data at their free will (for example, almost all apps read user's location). computation power and storage are implanted into or attached to a human body for data collection. The sensor wants to distribute its collected data securely to authorized doctors and other experts. The only thing that the sensor needs to know is that the doctor or expert has the privilege to access its data. There is no need for the sensor to know in detail who the doctor is. Meanwhile, the data produced may be requested by more than one authorized data consumer, as long as they all have the access privilege. To be more specific, we need a role-based access control. For example, the data produced by a sensor that monitors the ECG signal may only want the doctors in GWU hospital, Cardiac Surgery Center to read it, and there are many doctors that have the required property.

Moreover, the storage in a sensor is limited and the data collected should be stored in a data sink that has a larger storage. As we mentioned before, a data sink might be compromised physically or virtually. Therefore we need to eliminate the trust we put on the data sink by encrypting the stored data at the data sink. Thus the data sink itself has no access to the original data: it is just a storage device and the only functionality required is to store and index the data. In this paper, we propose a framework that makes this scenario secure by designing a protocol that facilitates role based encrypted access control and reduces the trust we place on the data sink.

Our contribution can be summarized as follow:

- We propose a framework that enables authorized doctors and experts to access a patient's private medical information securely.
- Instead of using software or other mechanism to perform access control, we use encryption and signature method to provide a role-based encrypted access control. The sensor has the ability to control who has access to its data by constructing an access structure for the data.
- We minimize the trust that people usually put on the data sink by storing the data in ciphertext. The compromise of the data stored at the data sink does not necessarily indicate that the data is compromised.
- We evaluate the performance of the proposed scheme in terms of energy consumption and communication/ computation overhead.

2. RELATED WORK

In this section, we summarize the most relevant existing research along three lines: (1) securing individual (implantable) devices within a BAN; (2) securing the communications within a BAN; and (3) identity-based cryptography for BANs. To the best of our knowledge, no prior work investigated the security of communications between a BAN and its external users except [14] [15], with [14] focusing on securing the communications (data encryption, access control, and digital signature) between the data controller and an external user via fuzzy attribute-based encryption and [15] addressing self-protecting electronic medical records (EMRs) on mobile devices and offline communications using attribute-based encryption.

Individual BAN devices: Halperin et al. [16] analyzed the security and privacy properties of commercially available Implantable Cardiac Defibrillators (ICDs). They identified a number of radiobased attacks that could compromise the safety and privacy of a patient. Other studies also discussed potential security and privacy risks of Implantable Medical Decives (IMDs) [17] [18] [19]. The existing research in this category is orthogonal to our work presented in this paper, as we focus on securing BAN communications.

Within a BAN: Most existing work in this category focused on securing the transmissions between an implantable device and a BAN controller, which can be a mobile phone carried by the patient. There have been extensive research on leveraging a unique feature of BAN - i.e., its ability to detect/measure vital signs such as inter-pulse-intervals (IPIs) - to establish secret keys and thereby enable secure communications within a BAN [7], [8], [9],[10], [11], [12]. In particular, since the IPI reading of a patient is measurable and fairly consistent over different places of the body, and generally differs substantially from other patients, most existing work assumed that IPI can be retrieved by all body sensors and used as a unique random number generator for cryptographic schemes (after a de-noising procedure such as).

Identity-based cryptography: With identity-based cryptography, the public key of each user can be easily computed from a string corresponding to the user's identity. Since this eliminates the cost of certificate distribution, identity-based cryptography is especially suitable for BANs.

Tan et al. [21] proposed an identity-based encryption scheme for BANs. Nonetheless, it lacks the access control feature which we develop in it. Yu et al. developed a distributed fine-grained access-control mechanism for wireless sensor networks. But it does not provide message authentication – another important requirement of BAN security.

3. SYSTEM MODEL

In this paper, we consider a BAN communication system depicted in Fig. 1. There are four major entities in this system: Key Generation Center (KGC), Sensor (implanted and wearable devices), Data Sink (the BAN data controller or a mobile device such as a smart phone), and Data Consumer (doctors or nurses). In the following subsections, we summarize the major functions of each entity. In this paper, we consider a BAN communication system depicted in Fig. 1. There are four major entities in this system: Key Generation Center (KGC), Sensor (implanted and wearable devices), Data Sink (the BAN data controller or a mobile device such as a smart phone), and Data Consumer (doctors or nurses). In the following subsections, we summarize the major functions of each entity.

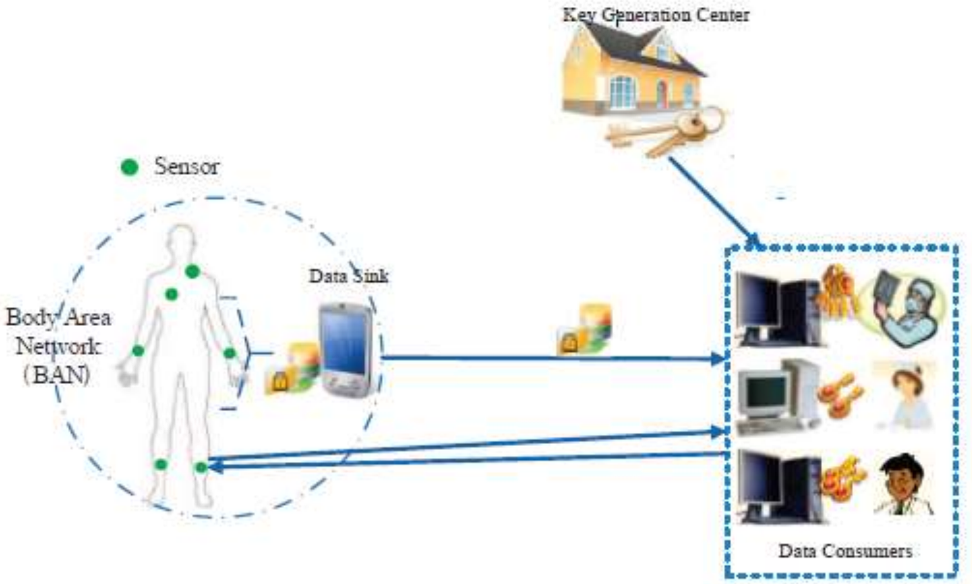

Fig. 1. A BAN architecture of a health care application

3.2.1 The Key Generation Center (KGC)

The KGC is used to perform system initialization, generate public parameters, and assign a secret key for each of the attributes a data consumer claims to have. The public parameters should be installed into the sensors before they are deployed (attached to or implanted in a human body) in a BAN. A data consumer should be able to prove to the KGC that it is the owner of a set of attributes and the KGC will generate a secret key for each attribute. One can see that the secret keys are uniquely generated for the data consumer, which implies that random numbers need to be associated with the set of secret keys to prevent collusion attacks. Sensors have all public parameters, which means that each sensor can construct an access tree and encrypt its data according to the access tree. Once a data consumer's attributes satisfy the access tree, it should be able to decrypt the message using the corresponding secret keys.

3.2.2 Implanted and Wearable Sensors

A BAN consists of wireless sensors called BAN devices either embedded on/near the surface (i.e., wearable devices) or implanted in the deep tissue (i.e., implanted devices) of a human body. These sensors are exploited to monitor vital body parameters or body movements (e.g., endoscopy capsules and motion sensors), and/or control the human body by providing life support, visual/audio feedback, etc. A BAN can be used by its human bearer for a variety of applications, including health care, military combat support, and athletic training, just to name a few. Implanted devices suffer from extremely restricted resources in terms of battery power, storage, and computation capability. Wearable devices, on the other hand, have much less stringent resource constraints. They are usually battery-powered and the batteries can be changed/recharged relatively easily. Wearable Example wearable devices include the sensors monitoring the cardiovascular system (electrodes on the chest to capture ECG, Peizo sensors on the wrist to measure blood pressure, optical sensors on the toe and earlobe to measure the pulse rate, microphones on the chest to measure heart sounds, etc.), the motion sensors placed on knees or in shoes, small cameras or video cameras attached to the sunglasses, and radars attached to the clothes or the stick to assist visually-disabled persons, etc.

The BAN devices should have certain computation capability to encrypt the patient’s data and store the ciphertext into the data sink. When a doctor or a nurse needs the data, she/he needs to communicate with the data sink to retrieve the (encrypted) data.

3.2.3 Data Sink

A data sink, which could be the BAN controller or a mobile device such as a smartphone, is used to store the patient’s data. We apply the attribute-based encryption proposed by Bethencourt, Sahai, and Waters [1] to encrypt the data and store the ciphertext in the data sink according to the requirements of the BAN. After data consumers retrieve a data item from the data sink, they can decrypt the data as long as they possess the secret key for the corresponding attributes specified by the access tree of the data. In a traditional framework, the data sink is used to authenticate the identity of a data consumer, verify its authorization status, retrieve and encrypt the data requested (with the keys shared by the data consumer and the data sink), and then send the data to the data consumer. Thus the data sink plays a vital role and we have to completely trust it. In other words, if we employ a mobile device such as a smartphone with a database that enables role-based access control as the data sink, we need to trust the smartphone to authenticate the data consumer, check the data consumer’s privilege, and establish a secure channel with the data consumer. If the smart phone is physically stolen or lost, the attacker can retrieve the data by analyzing the memory or disk. On the other hand, some applications in a smartphone often cross the line to collect unnecessary data, making such a data sink even more vulnerable to various attacks. In our framework, we leverage the fact that CP ABE can enable sensors to store the data in ciphertext; thus the data sink itself has no access to the original data. The only requirement for the data sink is to functionally store the encrypted data and disseminate the data to the data consumers that make requests. By this way we minimize the trust we usually put on the data sink. Therefore if we use a smartphone to store the data, the curious applications that intend to learn the data can obtain only the encrypted version. Based on the above analysis, in this study we assume that the data sink is honest but curious and easy to be compromised.

3.2.4 Data Consumers (DCs)

Data Consumers refer to the doctors and nurses or other experts. To decrypt a message, data consumers should have the attributes that satisfy the access tree specified by the data source. When the first time a data consumer joins the system, he needs to contact the KGC to obtain the secret key corresponding to the attributes he claims to have. The detailed method that shows how the data consumer can prove to the KGC that he possesses a set of attributes is out of the scope of this paper. For example, a data consumer can go to the KGC office and prove to the officer that he is a doctor in both GWU hospital and Cardiac Surgery Center. Then the KGC should generate a unique set of secret keys for the data consumer. One should notice that the secret keys are the crux to decrypt a message, not the attributes themselves. Attributes are public parameters and everyone could possibly know them. The secret keys for a data consumer are uniquely generated by KGC, which typically associates a random number with each key, to enable.

4. CONCLUSION AND FUTURE WORK

The proposed an efficient attribute-based encryption and signature scheme, which is a one-to-many encryption method. In other words, the message is meant to be read by a group of users that satisfy certain access control rules in a BAN. Meanwhile, we design a protocol to secure the data communications between implanted /wearable sensors and the data sink/data consumers. Our future research lies in the following directions: design a more efficient encryption approaches with less computation and storage requirement (CP ABE with constant ciphertext length), which could be better suitable for practical situations (the multiauthority CP ABE scheme) in BAN. However, there are extra computation cost in multi-authority CP ABE scheme and CP ABE with constant ciphertext length. The challenge is how to reduce the computation cost for better use in BAN. Note that the communication architecture for BAN proposed in this paper serves at the basis of our future research and we shall further propose new approaches to enhance and extend this architecture.

5.REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in Proceedings of the 2007 IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[2] 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. ACM, 2013, pp. 31– 36.

[3] D. Panescu, “Emerging technologies [wireless communication systems for implantable medical devices],” Engineering in Medicine and Biology Magazine, IEEE, vol. 27, no. 2, pp. 96–101, 2008.

[4] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, “Exploiting prediction to enable secure and reliable routing in wireless body area networks,” in INFOCOM. IEEE, 2012, pp. 388–396.

[5] S. Ali, V. Sivaraman, and D. Ostry, “Zero reconciliation secret key generation for body-worn health monitoring devices,” in ACM Wisec. ACM, 2012, pp. 39–50.

[6] L. Shi, M. Li, S. Yu, and J. Yuan, “Bana: body area network authentication exploiting channel characteristics,” in ACM Wisec.ACM, 2012, pp. 27–38.

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

[8] K. Venkatasubramanian, A. Banerjee, and S. Gupta, “PSKA: Usable and secure key agreement scheme for body area networks,”IEEE Transactions on Information Technology in Biomedicine, vol. 14, no. 1, pp. 60–68, 2010.

[9] “EKG-based key agreement in body sensor networks,” in INFOCOM Workshops 2008. IEEE, 2008, pp. 1–6.

[10] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, “Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body,” in Parallel Processing Workshops, 2003 International Conference on, 2003, pp. 432–439.

[11] K. Venkatasubramanian, A. Banerjee, and S. Gupta, “Plethysmogrambased secure inter-sensor communication in body are networks,” in Military Communications Conferenc, 2008, pp. 1–7.

[12] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, “Opfka: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks,” in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2274–2282.

[13] S. Pirbhulal, H. Zhang, S. C. Mukhopadhyay, C. Li, Y. Wang, G. Li, W. Wu, and Y.-T. Zhang, “An efficient biometric-based algorithm using heart rate variability for securing body sensor networks,” Sensors, vol. 15,no. 7, pp. 15 067–15 089, 2015.

[14] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, “Body area network security: a fuzzy attribute-based signcryption scheme,”Selected Areas in Communications, IEEE Journal on, vol. 31, no. 9, pp. 37–46, 2013.

[15] J. Akinyele, M. Pagano, M. Green, C. Lehmann, Z. Peterson, and A. Rubin, “Securing electronic medical records using attribute-based encryption on mobile devices,” in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. ACM, 2011, pp. 75–86.

[16] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend,W. Morgan, K. Fu, T. Kohno, and W. Maisel, “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses,” in Proceedings of the 2008 IEEE Symposium on Security and Privacy, 2008, pp. 129–142.

[17] W. Maisel, M. Moynahan, B. Zuckerman, T. Gross, O. Tovar, D. Tillman, and D. Schultz, “Pacemaker and icd generator malfunctions,” JAMA: the journal of the American Medical Association, vol. 295, no. 16, pp. 1901–1905, 2006.

[18] D. Halperin, T. Kohno, T. Heydt-Benjamin, K. Fu, andW. Maisel, “Security and privacy for implantable medical devices,” Pervasive Computing, IEEE, vol. 7, no. 1, pp. 30–39, 2008.

[19] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, “Sok: Security and privacy in implantable medical devices and body area networks,” in Security and Privacy (SP), 2014 IEEE Symposium on. IEEE, 2014, pp. 524–539.

[20] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” in Proceedings of the 6th ACM conference on Computer and Communications Security, 1999, pp. 28–36.

[21] C. Tan, H.Wang, S. Zhong, and Q. Li, “Body sensor network security: an identity-based cryptography approach,” in Proceedings of the first ACM conference on Wireless network security, 2008, pp. 148–153.