International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 7, September - 2012

# BAN Group Device coupling based protected Sensor connection for Key Management

[1]Ravindar Thammadi [2]Prof. D. Jamuna [3]Prof.M.Srinivasulu [4]Naveen Thammadi

**Abstract:** Body Area Networks (BAN) is a key enabling technology in E-healthcare such as remote health monitoring. An important security issue during riding bootstrap phase of the BAN is to securely associate a group of sensor nodes to a patient, and generate necessary secret keys to protect the subsequent wireless communications.

A group of sensor nodes, having no prior shared secrets before they meet, establish initial trust through group device pairing (GDP), which is an authenticated group key agreement protocol. тhe legality of each member node can be visually verified by a human by the protected sensor.

**Logical Key Words:** Protocol, Remote, Healthcare, GDP, Wireless communications.

## 1. INTRODUCTION

Wireless body area networks (BAN) have emerged as an enabling technique for E-healthcare systems, which will revolutionize the way of hospitalization. BAN is composed of small wearable or implantable sensor Nodes that is placed in, on or around a patient's body, which are capable of sensing, storing, processing and transmitting Data via wireless communications.

In addition, a controller (a hand-held device like PDA or smart phone) is usually associated with the same patient, which collects, processes, and transmits the sensor data to the upper tier of the network for healthcare records. A typical structure of the BAN and its relationship with the E-healthcare system is depicted in Fig.1

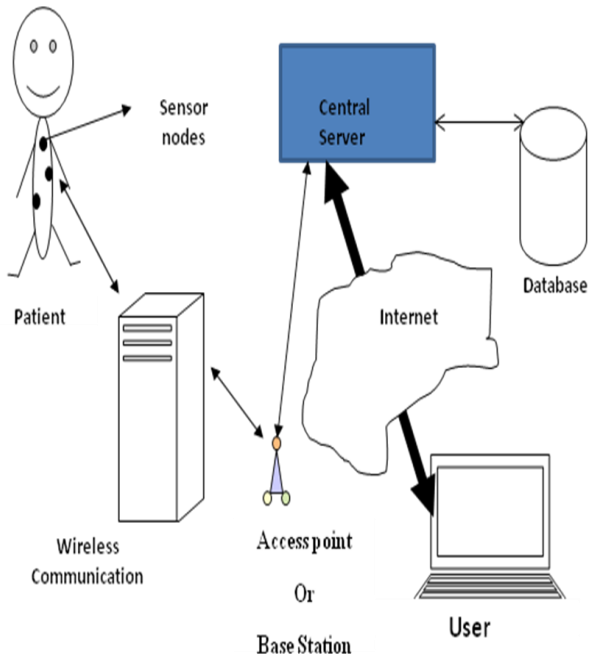


Fig 1Body area sensor network and Its relationship with the E-healthcare system.

The BAN is designed to satisfy a wide range of applications, such as ubiquitous health monitoring (UHM) and emergency Medical response (EMS) The UHM features longterm and consistent monitoring of a patient's health status and surrounding environment, while the EMS requires real-time medical data collection and reporting. Unlike conventional sensor networks, a BAN deals with more important medical information which has more stringent requirements for security. Especially, secure BAN bootstrapping is essential since it secures the very first step. In this paper we focus on the secure sensor association problem during BAN bootstrapping (before the BAN is actually deployed).

## 2. SERVER – DATA - USER MANAGEMENT

In order to achieve secure, scalable and fine-grained access control on outsourced data in the cloud, we utilize and uniquely combine the following three advanced cryptographic techniques: KP-ABE, PRE and lazy re-encryption. More specifically, we associate each data file with a set of attributes, and assign each user an expressive access structure which is defined over these attributes. To enforce this kind of access control, we utilize KP-ABE to escort data encryption keys of data files. Such a construction enables us to immediately enjoy fine-graininess of access control. However, this construction, if deployed alone, would introduce heavy computation overhead and cumbersome online burden towards the data owner, as he is in charge of all the operations of data/user management. Specifically, such an issue is mainly caused by the operation of user revocation, which inevitably requires the data owner to re-encrypt all the data files accessible on the leaving user, or even needs the data owner to stay online to update secret keys for users. To resolve this challenging issue and make the construction suitable for cloud computing, we uniquely combine PRE with KP-ABE and enable the data owner to delegate most of the computation intensive operations to Cloud Servers without disclosing the underlying file contents. Such a construction allows the data owner to control access of his data files with a minimal overhead in terms of computation effort and online time, and thus fits well into the cloud environment. Data confidentiality is also achieved since Cloud Servers are not able to learn the plaintext of any data file in our construction. For further reducing the computation overhead on Cloud Servers and

thus saving the data owner's investment, we take advantage of the lazy re-encryption technique and allow Cloud Servers to "aggregate" computation tasks of multiple system operations. As we will discuss in section V-B, the computation complexity on Cloud Servers is either proportional to the number of system attributes, or linear to the size of the user access structure/tree, which is independent to the number of users in the system. Scalability is thus achieved. In addition, our construction also protects user access privilege information against Cloud Servers. Accountability of user secret key can also be achieved by using an enhanced scheme of KP-ABE.

## 3. TECHNIQUE PRELIMINARIES

*A. Key Policy Attribute-Based Encryption (KP-ABE)*

*B. Proxy Re-Encryption (PRE)*

## 4 . Protected Sensor Connection and Key Management for BAN

1) Pre-deployment. In this phase, the sensor nodes are bootstrapped for the first time after purchased by the user or owner. This phase is assumed to be immune of node compromise, which allows the user to securely associate the sensor nodes to a patient. Group device pairing is performed among the sensor nodes and the controller to setup a group key. Also, keying materials are distributed by the controller to each sensor node using the group key.

2) Deployment. Nodes are actually deployed to designated places on/in/around the human body. Neighbor discovery is performed to form a BAN topology, pair wise keys are computed, and a logical key hierarchy is established.

3) Working phase, when the regular functions (e.g. collecting and reporting medical data) are executed. Our scheme updates all the keys periodically, and handles node join/leave /revocation efficiently.

## 5. IMPLEMENTATION

We implemented GDP on a sensor network platform consisting of 10 Tmote-Sky nodes, each with 8MHz TI-MSP430 microcontroller, 10KB RAM and 48KB Flash (ROM). We let one of the sensor nodes be the controller, which does not improve the performance of GDP protocol. The counting step is omitted, by programming the group IDs of sensor nodes and the group size into them in advance.We convert the Diffie-Hellman based group key agreement (UDB) to its elliptic curve cryptography (ECC) version, where the modular exponentiation and modular

multiplication correspond to point multiplication and point addition, respectively. We use the primitive operations provided by TinyECC including point multiplication and point addition, with all optimizations enabled.

## 6. CONCLUSION

In this paper, we propose a novel protocol, group device pairing (GDP), for secure sensor association and key management in BAN. A group of nodes and a controller that may have never met before and share no pre-shared secrets, form a group securely to associate to the correct patient. For each subgroup, GDP achieves authenticated group key agreement by simultaneously and manually compare the LED blinking patterns on all nodes, which can be done within 30 seconds with enough security strength in practical applications. GDP helps the user of BAN to visually make sure that the BAN consists only of those nodes that s/he wants to associate with the patient. The resulting group keys enable efficient key management after network deployment. Experimental results show that GDP greatly reduces the total time and complexity of human interactions, while being efficient both in communication and computation.

## 7. ACKNOWLEDGEMENT

The authors express their deep gratitude to the Principal and the Management members of JPNCE for their encouragement and extensive support in preparing and publishing of this paper.

## 8. REFERENCES

[1] M. Li, W. Lou, and K. Ren, "Secure device pairing," in Encyclopedia of Cryptography and Security (2nd Ed.), H. Tilborg and S. Jajodia Ed., Springer, to appear, 2010.

[2] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: an identity-based cryptography approach," in ACM WiSec '08:, 2008, pp. 148–153.

[3] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Key agreement in peer-to-peer wireless networks," Proceedings of the IEEE, vol. 94, no. 2, pp. 467–478, Feb. 2006.

[4] S. L. Keoh, E. Lupu, and M. Sloman, "Securing body sensor networks: Sensor association and key management," *IEEE* PerCom '09, pp. 1–6, 2009.

[5] S. Laur, N. Asokan, and K. Nyberg, "Efficient mutual data authentication using manually authenticated strings," in Cryptology and Network Security. Springer, 2005, pp. 90–107.

[6] P. Zimmermann, A. Johnston, and J. Callas, "Zrtp: Extensions to rtp for diffiehellman key agreement for srtp draft-zimmermann-avt-zrtp-01," in Internet-draft, March. 2006.

[7] R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," IEEE Trans. on Inf. Theory, vol. 54, no. 5, pp. 2007–2025, May 2008.

[8] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in CRYPTO '92. Springer-Verlag, 1993, pp. 471–486.

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

[10] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," SIGCOMM Comput. Commun. Rev., vol. 28, no. 4, pp. 68–79, 1998.

[11] K. Van Laerhoven, A. Schmidt, and H.-W. Gellersen, "Multi-sensor context aware clothing," in Wearable Computers, 2002. (ISWC 2002), 2002, pp. 49–56.

[12] S. Zhu, S. Setia, and S. Jajodia, "Leap: efficient security mechanisms for largescale distributed sensor networks," in *CCS '03*, 2003, pp. 62–72.

[13] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography
in wireless sensor networks," in *IPSN '08*, 2008, pp. 245–256.

**Authors:**

**1. Mr.Ravindar Thammadi,** Pursuing M.Tech(CSE) of CSE Dept. Jayaprakash Narayan College of Engg, Mabubnagar, M.Sc.Tech Applied Electronics from Osmania University. His areas of Interest

are in UML, Computer and Communication Networks, Computer Graphics, and Advanced Computer Architectures.

**2.Prof.D.Jamuna**, Working as Professor & Head of CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar, M.Tech(SE) from School of

Information Technology, JNTUH, Hyderabad. BE(CSE) from Vijayanagara Engineering College, Bellary. Experience 17 Years in Teaching Profession. Her areas of Interest are in Wireless Sensor Networks, Data Mining, Networking and guided M. Tech and B. Tech Students IEEE Projects. She is a Member of CSI.

**3.Prof. M Srinivasulu,** B.Tech., M.Tech., MISTE, MIE. Working as Professor & Head of ECE Dept. Jyothishmathi Institute of Technology and Science,Karimnagar. His areas of Interest are in Signal Processing.

**4.Dr.NaveenThammadi,** Pursuing M.D in forensic medicine from Kakatiya Medical College Warangal.MBBS from Osmania Medical College,Hyderabad. His areas of Interest are in forensic medicine.