International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Efficient Certificate less Access Control for Wbans

Student Name: SYED IBRAHEEM
M.Tech (CNIS) (15646D7803)
Mail id:syedibraheem50@gmail.com
Contact: 9885886513
GUIDE NAME: Mrs.M Shirisha (asst.prof), CSE
Mail id:shirishamara27@gmail.com
Hod name: Prof.V.Janaki Garu
Principal: PROF.P Prakash Garu
DEPARTMENT OF COMPUTER SCIENCE ENGINEERING
VAAGDEVI COLLEGE OF ENGINEERING

ABSTRACT

Wireless body area networks (WBANs) are expected to act as an important role in monitoring the health information and creating a highly reliable ubiquitous healthcare system. Since the data collected by the WBANs are used to diagnose and treat, only authorized users can access these data. Therefore, it is important to design an access control scheme that can authorize, authenticate, and revoke a user to access the WBANs. In this paper, we first give an efficient certificate less signcryption scheme and then design an access control scheme for the WBANs using the given signcryption.Our scheme achieves confidentiality, integrity, authentication, non-repudiation, public verifiability, and cipher text authenticity. Compared with existing three access control schemes using signcryption, our scheme has the least computational cost and energy consumption for the controller. In addition, our scheme

has neither key escrow nor public key certificates, since it is based on certificate less cryptography.

Wireless body area networks, security, access control, signcryption, certificate less cryptography.

INTRODUCTION

With the rapid progress in wireless communication and medical sensors, wireless body area networks (WBANs) are under rapid research and

Development. A typical WBAN is composed of a number of implantable or wearable sensor nodes and a controller. The sensor nodes are responsible for

monitoring a patient's vital signs (e.g. electrocardiogram, heart rate, breathing rate and blood pressure) and environmental parameter (e.g. temperature, humidity and light). The sensor nodes communicate with the controller and the controller acts as a gateway that sends the collected health data to the healthcare staffs and network servers. The WBANs increase the efficiency of healthcare since a patient is no longer required to visit the hospital frequently. The clinical diagnosis and some emergency medical response can also be realized by the WBANs. Therefore, the WBANs act as an important role in creating a highly reliable ubiquitous healthcare system. A good survey about the current state-of-art of WBANs is given by Movassaghi et al.

Since collected data by the WBANs act as a vital role in the medical diagnosis and treatment, only authorized users can access these data. Therefore, it is important to design an efficient access control scheme that is capable of authorizing, authenticating and revoking a user to access the WBANs. Without this access control, the health data may be abused, which may result in a catastrophic consequence. However, it is not an easy thing to design an efficient access control scheme for the WBANs because the resource of the sensor nodes is very limited. We give a CLSC scheme with public verifiability and cipher text authenticity. We design an access control scheme for the WBANs using the CLSC with public verifiability and cipher text authenticity. Our scheme achieves confidentiality, integrity, authentication, non-repudiation, and public verifiability and cipher text authenticity. In addition, the proposed scheme has neither key escrow problem nor public key certificates. The controller can verify the validity of a cipher text without decryption. Compared with existing three access control schemes using signcryption, our scheme has the least computational cost and energy consumption for the controller.

2. LITERATURE SURVEY

1) Low-SAR path discovery by particle swarm optimization algorithm in wireless body area networks

AUTHORS: T. Y. Wu and C. H. Lin

Sensor nodes in wireless body area networks are placed on the surface of the human skin or embedded inside the human body. When a transmitter sends packets, signals reach the receiver through the human body or skin. However, electric and

magnetic field (EMF) radiation generated during packet transmission can lead to a negative influence on human health. The specific absorption rate (SAR) is defined as a measure of the amount of radio frequency energy absorbed by human tissue in units of mass. The higher the human body absorbs the value of the specific absorption rate, the more EMF radiation. Also, the degree of harm to human health is greater. This paper uses the particle swarm optimization algorithm to discover the optimal position of the relay node so that sensor nodes can send packets to the hub via the relay node through a path with the lowest SAR and the success rate of packet transmission thus can be improved.

2) Energy efficient transmission approach for WBAN based on threshold distance

AUTHORS: C. Yi, L. Wang, and Y. Li

Energy efficiency is a key concern for wireless sensor nodes, especially for wireless body area network (WBAN) in which sensors operate in close vicinity to, on or even inside a human body. In this paper, we first present a system-level energy consumption model associated with transmission distance d and transmission data rate over on-body wireless communication link. Then, based on the analysis of tradeoff between circuit energy and transmission energy on distance, a threshold distance d_{th} which is responsible for the proportion of transmission energy and circuit energy is derived for energy saving in WBAN. With the case of $d \leq d_{th}$, since circuit energy is comparable with transmission energy consumption, the total energy consumption can be saved by optimizing the transmission data rate R. Simulation results show that a 59.77% or even more energy saving is achievable using the optimized scheme, compared with baseline scheme. With $d > d_{th}$, since the total energy consumption is monotonically decreasing with respect to time t, an offline algorithm is applied to energy saving by prolonging transmission time within the deadline time. In addition, on the basis of the offline algorithm, a battery-aware transmission approach is presented for WBAN using battery electrochemical property. Experimental results show that, using the presented battery-aware approach, 71.05% and 60.81% energy saving can be obtained, in comparison with the baseline and offline schemes, respectively.

3) A cyber physical test-bed for virtualization of RF access environment for body sensor network

AUTHORS: J. He, Y. Geng, Y. Wan, S. Li, and K. Pahlavan

Performance evaluation of wireless access and localization is important for body sensor networks, as any defects in the design not only cause wastage of resources, but also threaten an individual's health and safety. The typical cyber methods, however, such as software simulation, often fail to accurately simulate the influence of hardware implementation. The traditional physical methods, however, such as field testing, are not capable of creating repeatable and controllable channel conditions. To combine cyber and physical factors as well as to address the issue, we present a cyber physical test-bed for environment virtualization to facilitate the performance evaluation of wireless access and localization in body sensor networks. This test-bed creates a virtualized environment by emulating the wireless channel in a cybernetic way using a real time channel emulator. The original devices or systems under testing can be physically connected to a channel emulator to evaluate the performance in the virtualization environment. Furthermore, the cyber physical test-bed supports various scenarios from in-body data transmission to time of arrival based indoor localization. To validate the cyber physical approach, emulated outputs are compared with the empirical data obtained from actual measurements. To overcome the bandwidth limitation of traditional digital channel emulators, we have designed an analog channel emulator for UWB technologies. The preliminary verification of this analog emulator is introduced at the end of this paper.

4) WBANs-Spa: An energy efficient relay algorithm for wireless capsule endoscopy

AUTHORS: D. Liu, Y. Geng, G. Liu, M. Zhou, and K. Pahlavan

Wireless Body Area Networks (WBANs) are specific purpose sensor networks designed to operate autonomously to connect various medical sensors, located inside and outside of a human body. WCE quickly becomes one of the most popular WBANs applications. Due to finite energy budget of sensor nodes, transmission power should be as low as possible in order to increase the life time of WBANs. To this end, we addressed a relay network model from in body Wireless Capsule Endoscopy (WCE), to on-body relay nodes, and finally to external Access Point (AP) for the energy-efficient of WBANs in

heterogeneous environment for realistic medical applications. Also, we proposed WBANs-Shortest Path Algorithm (WBANs-Spa) of relay network to reduce total network power consumption using empirical path loss model, which could find the optimal multi-hop path based on the network model. Simulation results showed our design was effective for minimizing total network energy consumption in relay network for WBANs, and the effect of on-body relay nodes and external AP deployment was provided.

5) A novel and lightweight system to secure wireless medical sensor networks

AUTHORS: D. He, S. Chan, and S. Tang

Wireless medical sensor networks (MSNs) are a key enabling technology in e-healthcare that allows the data of a patient's vital body parameters to be collected by the wearable or implantable biosensors. However, the security and privacy protection of the collected data is a major unsolved issue, with challenges coming from the stringent resource constraints of MSN devices, and the high demand for both security/privacy and practicality. In this paper, we propose a lightweight and secure system for MSNs. The system employs hash-chain based key updating mechanism and proxy-protected signature technique to achieve efficient secure transmission and fine-grained data access control. Furthermore, we extend the system to provide backward secrecy and privacy preservation. Our system only requires symmetric-key encryption/decryption and hash operations and is thus suitable for the low-power sensor nodes. This paper also reports the experimental results of the proposed system in a network of resource-limited motes and laptop PCs, which show its efficiency in practice. To the best of our knowledge, this is the first secure data transmission and access control system for MSNs until now.

3. a) SYSTEM MODEL

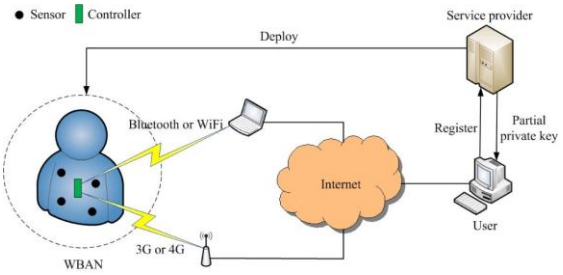

Fig. 1 shows the overview of the network model that mainly consists of three entities, the WBAN of a patient, a service provider (SP) and a user (e.g., a nurse, a doctor, a government agency or an insurance company). The WBAN consists of some sensor nodes and a controller. The

sensor nodes can communicate with the controller and the controller can communicates with not only the sensor nodes but also the Internet. The SP deploys the WBAN that monitors a patient's vital signs and environmental parameter. If a user hopes to access the WBAN, it must be authorized by the SP. The SP is responsible for the registration for both the user and the WBAN and producing a partial private key for the user and the private keys for the WBAN. That is, the SP plays the KGC in the CLC. We suppose that the SP is honest and curious (the SP follows the protocol but hopes to know the transmitted messages). That is, we do not need to fully trust the SP since it only knows the partial private key of the user. This is an important advantage of the CLC than the IBC. When a user hopes to access the monitoring data of the WBAN, it first sends a query message to the WBAN. Then controller checks if the user has been authorized to access the WBAN. If yes, the controller sends collected data to the user in a secure way. Otherwise, the controller refuses the query request.

B. Security Requirements

The communication between the user and the controller should satisfy at least four security properties, i.e. confidentiality, authentication, integrity and non-repudiation. Confidentiality keeps query messages secret from the others except the user and the controller. Authentication ensures that only the authorized user can access the WBAN. Integrity ensures that a query message from the user has not been altered by some unauthorized entities. Non-repudiation prevents the denial of previous queries submitted by the user. That is, if the user has submitted a query message to the WBAN, it cannot deny its action. In addition, we also hope that this communication satisfies public verifiability and cipher text authenticity. The public verifiability means that a third party can verify the validity of a cipher text without knowing the controller's private key. The cipher text authenticity means that a third party can verify the validity of a cipher text without decrypting it.

B. Motivation and Contribution

The previous access control schemes using signcryption have the following weaknesses: (1) they either require the public key certificates or have key escrow problem. (2) They do not have cipher text authenticity. The controller must first decrypt a cipher text and then verify its validity. If the cipher text is not valid, the decryption work will be wasted. The motivation of this paper is to find a new methodology for design of an access

control scheme for the WBANs without the above weaknesses. Only authorized users can access the WBANs and the query messages are protected. It is important to protect the query messages for preserving the privacy of the users [21]. Our methodology uses certificate less signcryption (CLSC) [22] with public verifiability and cipher text authenticity. The contributions of this paper are summarized as follows

1) We give a CLSC scheme with public verifiability and cipher text authenticity.
2) We design an access control scheme for the WBANs using the CLSC with public verifiability and cipher text authenticity. Our scheme achieves confidentiality, integrity, authentication, non-repudiation, public verifiability and ciphertext authenticity. In addition, the proposed scheme has neither key escrow problem nor public key certificates. The controller can verify the validity of a ciphertext without decryption. Compared with existing three access control schemes using signcryption, our scheme has the least computational cost and energy consumption for the controller.

4. CONCLUSION

In this paper, we proposed a modified certificate less signcryption scheme that satisfies public verifiability and cipher text authenticity. We also gave a certificate less access control scheme for the WBANs using the modified signcryption. Compared with existing four access control schemes using signcryption, our scheme has the least computational time and energy consumption. In addition, our scheme is based on the CLC that has neither key escrow problem nor public key certificates.

5. REFERENCES

[1] T. Y. Wu and C. H. Lin, "Low-SAR path discovery by particle swarm optimization algorithm in wireless body area networks," IEEE Sensors J., vol. 15, no. 2, pp. 928–936, Feb. 2015.

[2] C. Yi, L. Wang, and Y. Li, "Energy efficient transmission approach for WBAN based on threshold distance," IEEE Sensors J., vol. 15, no. 9, pp. 5133–5141, Sep. 2015.

[3] J. He, Y. Geng, Y. Wan, S. Li, and K. Pahlavan, "A cyber physical test-bed for virtualization of RF access environment for body sensor network," IEEE Sensors

J., vol. 13, no. 10, pp. 3826–3836, Oct. 2013.

[4] D. Liu, Y. Geng, G. Liu, M. Zhou, and K. Pahlavan, "WBANs-Spa: An energy efficient relay algorithm for wireless capsule endoscopy," in Proc. IEEE 82nd Veh. Technol. Conf. (VTC-Fall), Boston, MA, USA, Sep. 2015, pp. 1–5.

[5] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," IEEE J. Biomed. Health Inform., vol. 18, no. 1, pp. 316–326, Jan. 2014.

[6] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1658–1686, Jan. 2014.

[7] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Commun., vol. 17, no. 1, pp. 51–58, Feb. 2010.

[8] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Secur. Privacy (HotWiSec), Budapest, Hungary, 2013, pp. 31–35.

[9] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[10] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 3, pp. 614–624, Mar. 2013.

[11] H. Zhao, J. Qin, and J. Hu, "An energy efficient key management scheme for body sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2202–2210, Nov. 2013.

[12] D. He, S. Chan, Y. Zhang, and H. Yang, "Lightweight and confidential data discovery and dissemination for wireless body area networks," IEEE J. Biomed. Health Inform., vol. 18, no. 2, pp. 440–448, Mar. 2014.

[13] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-Lite: A lightweight identity-based cryptography for body sensor networks," IEEE Trans. Inf. Technol.

Biomed., vol. 13, no. 6, pp. 926–932, Nov. 2009.

[14] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.

[15] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 332–342, Feb. 2014.

[16] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 2894. New York, NY, USA: Springer-Verlag, 2003, pp. 452–474.

[17] G. Cagalaban and S. Kim, "Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption," in Proc. 13th Int. Conf. Adv. Commun. Technol. (ICACT), Seoul, Korea, Feb. 2011, pp. 863–867.

[18] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3386. New York, NY, USA: Springer-Verlag, 2005, pp. 362–379.

[19] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) cost(signature) + cost(encryption)," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 1294. New York, NY, USA: Springer-Verlag, 1997, pp. 165–179.

[20] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: A fuzzy attribute-based signcryption scheme," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 37–46, Sep. 2013.

[21] C. Ma, K. Xue, and P. Hong, "Distributed access control with adaptive privacy preserving property for wireless sensor networks," Secur. Commun. Netw., vol. 7, no. 4, pp. 759–773, Apr. 2014.

[22] P. S. L. M. Barreto, A. M. Deusajute, E. de Souza Cruz, G. C. F. Pereira, and R. R. da Silva, "Toward efficient certificateless signcryption from (and without) bilinear pairings," in Proc. Brazilian Symp. Inf. Comput. Syst. Secur., 2008, pp. 115–125.

[23] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3788. New York, NY, USA: Springer-Verlag, 2005, pp. 515–532.

[24] C. P. Schnorr, "Efficient signature generation by smart cards," J. Cryptol., vol. 4, no. 3, pp. 161–174, 1991.

[25] S. S. M. Chow, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," in Information Security and Cryptology (Lecture Notes in Computer Science), vol. 2971. New York, NY, USA: Springer-Verlag, 2004, pp. 352–369.

[26] C. Gamage, J. Leiwo, and Y. Zheng, "Encrypted message authentication by firewalls," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 1560. New York, NY, USA: Springer-Verlag, 1999, pp. 69–81.

[27] J. Daemen and V. Rijmen, The Design of Rijndael: AES—The Advanced Encryption Standard. Springer, 2002.

[28] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," Int. J. Inf. Secur., vol. 1, no. 1, pp. 36–63, Aug. 2001.

[29] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science), vol. 3156. New York, NY, USA: Springer-Verlag, 2004, pp. 119–132.

[30] K.-A. Shim, Y.-R. Lee, and C.-M. Park, "EIBAS: An efficient identitybased broadcast authentication scheme in wireless sensor networks," Ad Hoc Netw., vol. 11, no. 1, pp. 182–189, Jan. 2013.

[31] X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: Identity-based multiuser broadcast authentication in wireless sensor networks," Comput. Commun., vol. 31, no. 4, pp. 659–667, Mar. 2008.

[32] F. Li, Z. Zheng, and C. Jin, "Secure and efficient data transmission in the Internet of Things," Telecommun. Syst., vol. 62, no. 1, pp. 111–122, 2016.

[33] K. A. Shim, "S2DRP: Secure implementations of distributed

reprogramming protocol for wireless sensor networks," Ad Hoc Netw., vol. 19, pp. 1–8, Aug. 2014.

[34] K. Ren, W. Lou, K. Zeng, and P. J. Moran, "On broadcast authentication in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 6, no. 11, pp. 4136–4144, Nov. 2007.