

A Communication Security Protocol for Ubiquitous Sensor Networks

Mangal Sain, Ndibanje Bruce, Ki Hwan Kim, Hoon Jae Lee

Department of Computer Engineering, Dongseo University, Busan, South Korea

mangalsain1@gmail.com, bruce.dongseo.korea@gmail.com, gend90@gmail.com, hjee@dongseo.ac.kr,

Abstract— The data accessibility anytime and anywhere is nowadays the key feature for information technology enabled by the ubiquitous network system for huge applications. However, security and privacy are perceived as primary obstacles to its wide adoption when it is applied to the end user application. When sharing sensitive information, personal s' data protection is the paramount requirement for the security and privacy to ensure the trustworthiness of the service provider. To this end, this paper proposes communication security protocol to achieve data protection when a user is sending his sensitive data to the network through gateway. We design a cipher content and key exchange computation process. Finally, the performance analysis of the proposed scheme ensure the honesty of the gateway service provider, since the user has the ability to control who has access to his data by issuing a cryptographic access credential to data users.

Keywords— Communication Protocol, Gateway, Access Credential, Security, Privacy

I. INTRODUCTION

In most cases, user sensitive information such as biomedical data are progressively converted into digital form, and placed in databases and other repositories for ease of access by the appropriate parties. In case of ubiquitous network system for example: in a lot of countries, healthcare providers, medical practitioners are adopting Electronic Medical Record (EMR) systems, and large companies, such as Google and Microsoft are building medical record gateways (e.g. Google Health and Microsoft HealthVault).

The security approach of healthcare system can be summarized in number of ways; in this regard, we take in consideration as a holistic point of view where the system can be seen as an entity that consists of multiple users playing different roles linked with different responsibilities, and mutual interaction. Among user's records there are those classified top secret such as details of a user's disease, drug usage, sexual preferences, once they are disclosure to public can harm user life. In this situation, if any attacker can somehow capture user's data, he might upload and store the data to social websites like facebook and consequently pose risks to the user's privacy. In addition, there may be no means to repair such harm financially, socially or self-confidence of user.

The other security approach in USN can be analysed through RFID system which nowadays has a wide range of applications. Being into the field, the sensors are physically accessible very easy. This exposure raises the possibility of

sensor attack and gain access inside the memory for further dip attacks such key control attack. Key control protocol plays the role to construct safe communication infra and to create secret key that are necessary for various security protocols by establishing the reliable relationship between sensor nodes, which are temporarily installed under the condition without reliable sensor or infra [1]. As key control mechanisms, there are pairwise key, random key pre-distribution, public key infrastructure and hierarchical key management [2]. As a shared key in network, pairwise key is used in encoding and authentication, providing effectiveness and simplification. However, the damage caused by node capture may affect entire network, and thus, additional key renewal protocol is required [2], [3]. Before installation random key pre-distributions receive random number of keys from the previously created key pool. It uses the key if neighboring key and common key exist, but it establishes link key through the connected neighboring node if they do not exist.

The problem addressed in this paper is the confidentiality and trust of gateway providers by the customer. This paper considers a case of users who wants to upload their data to gateway but because of untrustworthiness, we propose a way where the user can encrypt their data before uploading it to gateway. Hence, the user would trust in the gateway infrastructure that supports critical applications for the ubiquitous system. The collected and stored data can be encrypted by the user and send to the gateway provider for future usage. The remainder of this paper is organized as follow; Section II presents the literature review. We develop our method in Section III and security analysis is given in Section IV before concluding in Section V.

II. LITERATURE REVIEW

Ling et al. [4] developed an improved Improvement of a Robust User Authentication Framework for Ubiquitous Sensor Networks. At first they established an analysis to the original protocol where they pointed out the weakness and proposed new enhancements. The mutual authentication process has drawbacks under the collusion attack. To enhance the original scheme, they bring a slight improvement into it while they have not made important impacts on the primary scheme. This improvement only needs to add a secret parameter into each sensor node.

Katsikas et al. [5] presented a security implementation where trusted third party (TTP) and its services are employed in distributed healthcare environment. The trusted third party mechanism certificates the interactions between two

participants. The two participants rely on their trusted party to secure their own interactions in order to achieve their goal.

The user centered access to secure systems online has been presented in [6]. The authors claim that, initially; it aims to permit users and health care providers to access health information, even the sensitive data. Their access scheme combines role-based access control, mandatory access control and discretionary access control. The implementation is a user-centered and centralized approach that stores all the data on a single server.

Different countries have developed and implemented their e-Healthcare System such as electronic Health Card (eHC) system [7] in German where each user has an eHC smartcard as described in the compulsory health insurance system. The main function of eHC is to store the administrative data (for billing with the health insurance), with embedded encryption operations of user's records to be saved on HER servers and to give access rights when the data is needed.

In practical case, once upon there is a need of patient's data, the data owner has to provide his eHC and also to enter a PIN to initiate encryption (upload) or to authorize access (download). Furthermore, in this system, for the authentication purpose as legitimate medical staff, the medical doctors possess their own smartcard, the Health Professional Card (HPC), which is also used to digitally sign documents that are stored in a patient's HER. Each health care provider has to have a special smartcard reader where the eHC and the HPC are inserted whenever access to the EHR is requested. A special connector locally interconnects the computing platforms of the health care provider with the smartcard reader and the telematics infrastructure. The connector is also used to connect to other networks that provide additional applications, but which are not part of the telematics system itself. The client platforms and the local networks of health care providers are out of scope of the healthcare telematics security requirements. In addition, when patients want to administer their personal data or manage access rights, they also need to use corresponding client platform systems. In both cases it is completely up to the end-users to secure their systems appropriately. Thus, the software on these computer systems can be identified to be the most likely attack target [8], as they are standard PC systems with commodity operating systems that offer standard services, e.g., e-mail and Internet access.

III. COMMUNICATION SECURITY PROTOCOL FOR UBIQUITOUS SYSTEM

The proposed access control scheme integrates a cryptographic function to render the whole communication process secure, hence data security and privacy are provided. The subsection in the next paragraph describes the design where the user data is encrypted with a secret key shared with the authorized person to decrypt the data. First we design the ciphertext content and second, the secret shared key computation is described.

The user using his secret key K encrypts his sensitive data let us call $\langle M \rangle$ the data obtained. From the user device, he encrypts and uploads the ciphertext to the system

$$EK(M) = C(M) \quad (1)$$

TABLE 1. Notations and Descriptions

Descriptions	Notations
Secret shared key	K
user Data(M) encrypted by K	$E_K(M)$
Cipher Text to sent to gateway	$C(M)$
gateway_ID	Idg
Nonce_gateway	Ng
Timestamp of gateway	Tg
User_ID	Idu
Nonce of user	Nu
Timestamp of user	Tu
Cryptographic hash function e.g. SHA1, SHA2	$h(.)$
Denotes concatenation operation	$\parallel$
Primitive element in the Galois field $GF(p)$	g

1) *Ciphertext component*: The content of the ciphertext $\{C(M)\}$ such as attributes, shared secrets keys and accessibility conditions will define the rights of the authorized devices to decrypt the data. If any attacker can access the encrypted data from the system he will not be able to read the content because restrictions access embedded into the cipher. Furthermore, shared secret keys are required to access the data. The involved entities in a given system are listed below but not exhaustive (in this paper we only focus on user and gateway as entities).

2) *Key Exchange Computation Procedures*. The ciphertext $C(M)$ stored by data owner contains the keys and they are computed into the system. They play vital role in our proposed method such as: mutual authentication, data access rights, encryptions and decryption. This paragraph describes the fundamental operations to compute the keys as given in the algorithm 1.

In this computation process, the user and gateway perform exponential calculations based on their identifications parameters. In this process, the long-term private keys are assigned to individual users and the secrets numbers are generated for each authenticated key exchange session. It is mathematically guaranteed that the confidentiality of the shared private keys is protected even if long-and secrets numbers are leaked in any combination (except in the case where both the long- and secrets numbers of the same user are compromised).

In addition to the public-key-based authenticated key exchange, where authentication is performed between user and gateway with public keys, there are also variants of authenticated key exchange such as a protocol where it is

possible that a shared private key is shared only when the other party fulfills certain specified conditions.

Once the shared keys computations between user and gateway are done, the encryption process of user data can start whenever the user wants to send to the system.

The other approach is to leverage enterprise rights management (ERM) to distribute the secret key K with licenses and distribute the licenses to list of recipients.

$$License \leftarrow (ID_i, PK_i, K, sigp, Policy) \quad (2)$$

Algorithm 1: Key Exchange Computation Algorithm

Required : User device, gateway

STEP I

Action : Long private key and public key computation

// Actions done by user

1: Compute $r = h(Id_u || Nu || Tu)$

2: Compute public key(gr) with r

3: Send gr to gateway and wait replies from gateway

// Actions done by Gateway

4: Compute $n = h(Id_g || Ng || Tg)$

5: Compute public key(gn) with n

6: Send gn to user device

STEP II:

Action : Compute short term public key and secret number

//Actions done by user device

7: Generate a secret number c

8: Compute short term key(gc) with c

9: Send gc to gateway and wait replies from gateway

// Actions done by gateway

10: Generate a secret number f

11: Compute short term key(gf) with f

12 : Send gf to user device

STEP III:

Action : Secret shared key computation

// Action by user device

13: Compute $K = (gn)y || (gf)y || (gn)c || (gf)c = gny || gfy || gnc || gfc$

//Action by gateway

14: Compute $K = (gr)n || (gr)f || (gc)n || (gc)f = gnr || gfr || gnc || gfc$

15: **End**

IV. SECURITY DISCUSSION

1) *The scheme is secure to chosen ciphertext-only attack:*

Data transmissions from user to gateway as well as from gateway to user are done with proper encryption. The processes are the same under Chosen Ciphertext Attack (CCA) [16] based on the modification of stored ciphertext to gateway. Such adversaries are permitted to see the ciphertexts for messages of their choice, and (in the public-key setting) to generate ciphertexts on their own. However, the adversary never gets to see the decryptions of any messages. For the reason that the credentials contain hashed secrets parameters

$r = h(Id_u || Nu || Tu)$ and $n = h(Id_g || Ng || Tg)$ to verify the authenticity of the attacker. Nonetheless, for some applications, the adversary will need a stronger definition in which he gets (limited) access to the decryption machinery as well.

2) *The scheme is resistant to the eavesdropping attack:*

The aim of an eavesdropping attacker is to have the access to the private and sensitive user's data. This attack may be happened between the involved entities during communication and exchange message. To access the data at the gateway server, an attacker needs to have sufficient attributes to complete the access authentication protocol process (step1, step2 and step 3 from the algorithm 1). Here the shared secret key is made by multiple secrets parameters based on the attributes set. For the non-privacy dataset, he may get access and allowed in our scheme. But he cannot modify the data due to the verification bindings. However, for the user sensitive data, a unique random number is embedded into the ciphertexts (Nu) and (Ng). Without knowing that secret number, it is impossible to access the data. Therefore, any attacker cannot successfully launch the eavesdropping even through sophisticated applications can do that.

3) *The scheme ensures message integrity, non-repudiation, and source authentication:* We use the user's secret key and the session identity to generate the signature playing the session key role $K = (gr)n || (gr)f || (gc)n || (gc)f$. The data receiver can verify the signature by using the public parameters of the sender "gc". This verification ensures the corresponding source authentication. The scheme computes secrets keys "n" and "r" by computing their hash values of the concatenated message. Only the user and gateway know each other their secrets keys which include the same of their attributes such Ids. With others subkeys, the secret key are also used to generate the signature "K". Therefore the message integrity with non-repudiation can be provided by our proposed scheme.

III.CONCLUSIONS

In this paper, we presented a communication security protocol for protecting sensitive data when using ubiquitous system. First, we defined the attributes of the involved entities in this paper and we described the contents of the ciphertext C (M) uploaded to gateway. Moreover, we presented the concept of credential based on the keynote trust management which provides the credentials functions. By the end, we made a security analysis regarding known attack to cipher and gateway storage, hence the proposed scheme have been founded efficient and resilient to various kinds of attacks.

ACKNOWLEDGMENT

This research was financially supported by the Ministry of Trade, Industry and Energy(MOTIE) of the Republic of Korea and Korea Institute for Advancement of Technology(KIAT) through the Regional Specialized Industry Development Program(Grant Number : R0005598).

This work is supported by Basic Science Research Program through the National Research Foundation of Korea

(NRF) funded by the Ministry of Education, Science and Technology. (Grant number: NRF-2011-0023076).

REFERENCES

- [1] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Network", Wireless Network Journal(WINE), September 2002.
- [2] W. Du, J. Deng, Y. S. Han and P. Varshney, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Network", 10th ACM Conference on Computer and Communications Security (CCS), October 2003.
- [3] J. Staddon, S. Miner, and M. Franklin, "Self-Healing Key Distribution with Revocation", Proceedings of 2002 IEEE Symposium on Security and Privacy (S&P2002), May 2002.
- [4] L. Chi, L. Hu, H. Li and J.Chu, " Analysis and Improvement of a Robust User Authentication Framework for Ubiquitous Sensor Networks." International Journal of Distributed Sensor Networks, Volume 2014, Article ID 637684, 6 Pages, Hindawi
- [5] S. K. Katsikas, D. D. Spinellis, J. Iliadis, and B. Blobel, "Using trusted third parties for secure telemedical applications over the WWW: The EUROMED-ETS approach", International Journal of Medical Informatics, 1998. 49(1): p. 59-68.
- [6] D. R. Masys and D. B. Baker. "user-Centered Access to Secure Systems Online (PCASSO): A Secure Approach to Clinical Data Access Via the World Wide Web". 1997.
- [7] Gematik. Einf uhrung der Gesundheitskarte - Netzwerkspezikation, Version2.0.0
http://www.gematik.de/upload/GA_ZentraleDienste_5171.zip, August 2009.
- [8] H.-H. Rau, C.-Y. Hsu, Y.-L. Lee, W. Chen, and W.-S. Jian. "Developing electronic health records in Taiwan". IT Professional, 12:17-25, 2010



ubiquitous sensor network/radio frequency identification security.

Hoon-Jae Lee received his BS, MS, and PhD. degrees in Electrical Engineering from Kyungpook National University, Daegu, South Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information and Communication Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His current research interests include developing secure communication system, side-channel attack, and



Mangal Sain received the M.Sc. degree in computer application from India in 2003 and the Ph.D. degree in computer science in 2011. Since 2012, he has been an Assistant Professor with the Department of Computer Engineering, Dongseo University, South Korea. His research interest includes wireless sensor network, cloud computing, Internet of Things, embedded systems, and middleware. He has authored over 30 international publications including journals and international conferences. He is a member of TIIS

and a TPC member in several international conferences



Bruce Ndibanje received the B.Sc degree in Computer Sciences, from Ngozi University, Burundi in 2006, the MS degree in Ubiquitous IT from Dongseo University in 2013. He has worked with many companies in the ICT domain such Huawei, United Nations, and Econet Wireless Burundi. Currently he is a Doctorate Researcher member of the Cryptography and Network Security Lab at Dongseo University, Busan, Korea since 2013. His research interest includes Wireless and

Sensor Networks, Authentication Protocol, Security in: e-Healthcare System, Cloud Computing and Cellular Networks, Side-channel attack and Countermeasures. He is a member of the IEEE Computer Society.



Ki Hwan Kim

2013: BS at Dongseo University, Republic of Korea
2015: MS at Dongseo University, Republic of Korea
2015 ~ current: doctor's course Dongseo University, Republic of Korea
Research Interests: Wireless Sensor Networks, Cryptography and Network Security, Side Channel Analysis