RESEARCH ARTICLE OPEN ACCESS

A New Secure Wireless Body Sensor Network Architecture

Kholoud Sweekat [1], Fatema Zarka [2], Boushra Maala [3], Ahmad S. Ahmad [4]
Third Year Student [1], Assistant Professor [4]
Faculty of Medical Engineering
Al-Andalus University, Al Qadmous - Tartus, Syria
Fourth Year Student [2], Assistant Professor [3]
Faculty of Mechanical and Electrical Engineering
Tishreen University, Lattakia
Syria

ABSTRACT

A wireless body sensor network (WBSN), is a network of sensors deployed on a person's body, usually for health care monitoring. Since the sensors collect personal medical data, security and privacy are important components in BSN. At the same time, the collected data has to readily available in the event of an emergency. In this paper, we present a new secure WBSN architecture for a BSN.

Keywords **:-** Wireless Body sensor network, Security, Privacy, Cryptography, RSA algorithm.

I. INTRODUCTION

Applying wireless sensors toward health care monitoring allows for new ways to provide quality health care to patients [1]. A diverse array of specialized sensors can be deployed to monitor, for instance, at-risk patients with history of heart attacks, or senior citizens living independently at home. These sensors provide continuous, long term monitoring in an unobtrusive manner, allowing doctors to diagnose problems more effectively.

The motivation behind a BSN is to place low cost sensors directly on the patient to collect physiological information for health care monitoring. It consists of sensors placed directly on a patient's body or woven into the patient's clothes and "travels" with the patient collecting data. The fact that a BSN is "always on", continuously collecting data, creates additional security and privacy demands. In fact, several research prototypes have been developed [2-6].

A patient will rightly want to limit the access and scope of the collected data to different people. For the purpose of this paper, we assume the patient wishes to control data access according to the date, time and the identity of the person who will access the data. Sensor network security is a widely researched area [6,7], with solutions focusing on key deployment [8-10], Public key cryptography [11] and management [12,13].

In this paper, we focus on a BSN deployed for medical monitoring. The data collected by the BSN can be stored in the sensors themselves, on a home computer, or forwarded to a publicly accessible website. We use the term storage site to refer to where the data is stored.

We consider an adversary that seeks unauthorized access to the patient's data so that, we need more protection and security for our network. This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

II. RELATED WORKS

We can provide the necessary security protections by designing the BSN to encrypt data with different keys.

A. Symmetric Key Encryption

In symmetric key encryption, the same key is used to both data encryption and decryption. So, for a patient wearing a BSN that monitors a patient 24h day for an entire month and only wants his primary doctor to access the information, will need to store 24*30*1=720 symmetric keys in the BSN, assuming that a different key is used every hour. If the patient wishes to control access to different people (others doctor and so on), then more keys will have to be assigned to the BSN. A problem occurs when the BSN or a single sensor from the BSN is stolen. When this happens, the adversary will be able to decrypt the data, since the same key is used for both encryption and decryption. One solution is to increase the number of encryption keys by letting each sensor use a different key to encrypt the data collected at the same time. For a BSN with 100 sensors, we will have 100*24*30*1= 72000 keys in the example given above. This makes key management complicated since the decrypting party may not know in advance which key is used. For this reason, many conventional protocols such as SSL on the Internet use symmetric keys to encrypt data, but use public keys to encrypt the symmetric key before transmission.

B. Asymmetric Encryption Key:

In conventional public key encryption like Rivest-Shamir-Adleman algorithm (RSA), two keys are used, an encryption key and a decryption key. Here, the encryption key is stored on the BSN, and the decryption key is stored safely elsewhere. When the BSN is compromised, the adversary will only learn the encryption key and cannot decrypt the data.

However, once the private key is revealed, all encrypted data is vulnerable. This poses a problem when temporary access to the BSN data is needed. For instance, consider an on duty doctor wanting to access the BSN data. If only one public key is used to encrypt all the data, the doctor after learning the private key will be able to decrypt all data even when he is off duty. A possible solution is to store many public keys in the BSN. However, this will also lead to similar key management problems as with symmetric key encryption.

III. OUR CONTRIBUTION

We design a system based on RSA algorithm and a storage site in order to provide security and privacy protections while allowing flexible access to stored data.

A. *RSA Algorithm*

It is one of the first puplic-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem".

The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption [14].

B. PROPOSED SYSTEM

Our research discusses how to communicate between the patient and the doctor and develop several ideas to achieve a secure and protected communication as much as possible. First, our WBSN network will be two-phases. Any communication between the patient and the doctor is not direct, but it is in two stages: the first stage between the patient and the storage site and the second between the storage site and the doctor. Let's illustrate the idea with the simple example below:

1-The information is collected on the body of the patient and then encrypted and sent to the storage site.

2- When message reaches the site which decrypts and reads it then it re-encrypts and sends it to the corresponding doctor.

3- When the doctor wants to send the reply message, he encrypts it and sends it to the storage site.

4- The site decrypts the reply message, reads and re-encrypts it in order to send it to the specified patient.

5- The message reaches the corresponding patient that decrypts and reads it and do what is necessary.

Thus, the operation was successful.

Patient ⇆ Storage site ⇆ Doctor.

C. OPERATION STEPS

Assume that:

1- The BSN network is a set of nodes, each sensor on the patient's body and each doctor connected to the network is a node.

2- The storage site is a sophisticated device that has key pairs (public-private) key for all nodes in the BSN network, and distributes keys and "ID Address" to each node, but in our research and to increase safety we distribute only the ID and public keys so that each node derives its own private key from the public it arrives. From this assumption, private keys are not accessed during distribution to the nodes. In addition, this site is completely protected and cannot be hacked.

3- Each node encrypts its information with the public key of the node to which it is sent and decrypts with own private key.

4- The process of distributing the keys and the ID is done offline and thus saving the energy which is very important.

5- The sensors collect data from the patient's body, then it encrypts it with the public key of the storage site and sends encrypted data to it, with the data the node sends the ID of the storage site and the ID of the concerned doctor so that when the storage site decrypt, it will able to know the destination to be sent back to. It is also the case for the doctor when he sends the reply message to the storage site that ensures the ID of the concerned patient.

Thus, we have achieved that every doctor is informed only of the patient's information that concerns him.

D. BSN Security and our Developments

To increase security in the network, we assume that the collection of information about the patient's body is 6 times per hour, so any message that arrives during these periods is safe otherwise it is unsafe. However, it is important to consider the patient's sudden condition. In this case, a specific agreement is made between the patient and the storage site according to the protocol used. Thus, the messages that are received during the specified and the unspecified periods but which include the agreement are secure messages, otherwise they are unsafe and are ignored.

If a member of the patient's family is always concerned about him and wants to inquire about his or her condition permanently, in this case we considered the new individual as a node in the network and gave him the authority to receive messages only. Suppose the new individual is node N:

The storage site distributes the public key to N, N derives its own private key from it. The site sends a reassurance message to N, encrypts it with the public key.

N decrypts the message with private key and rest assured on the condition of patient. The following charts illustrate the above-mentioned mechanism:

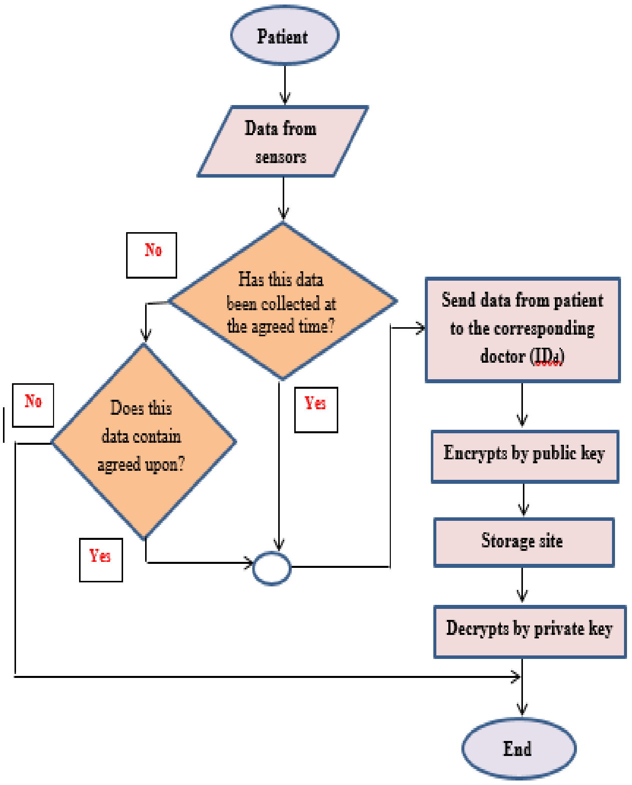
Patient
Data from sensors
No
Has this data been collected at the agreed time?
Send data from patient to the corresponding doctor (IDd)
No
Does this data contain agreed upon?
Yes
Encrypts by public key
Yes
Storage site
Decrypts by private key
End

Fig. 1 The mechanism from patient to storage site

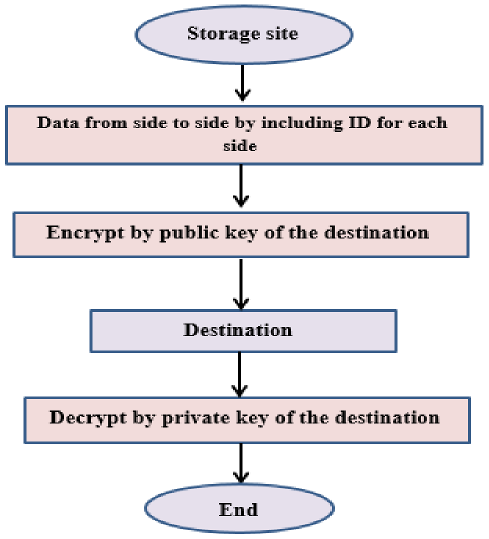
Storage site
Data from side to side by including ID for each side
Encrypt by public key of the destination
Destination
Decrypt by private key of the destination
End

Fig. 2 The mechanism from storage site to other side (patient or doctor)

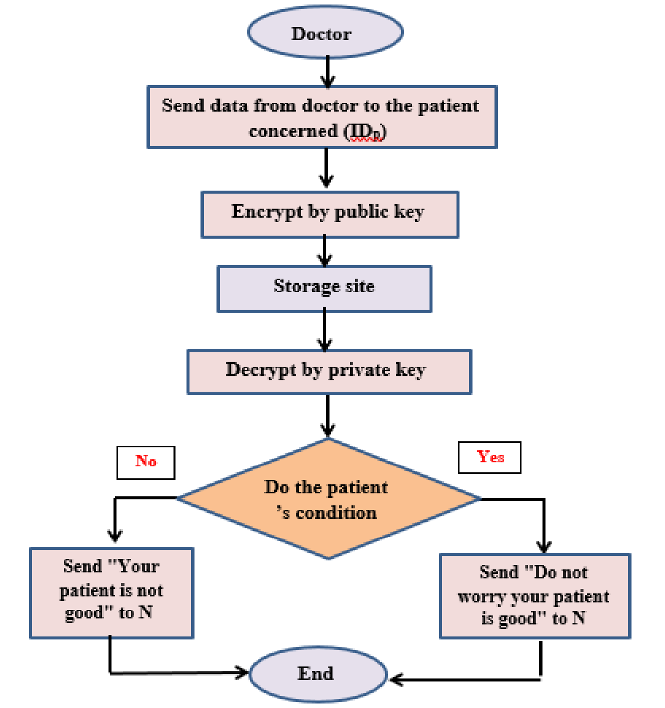
Doctor
Send data from doctor to the patient concerned (ID$_D$)
Encrypt by public key
Storage site
Decrypt by private key
No
Yes
Do the patient 's condition
Send "Your patient is not good" to N
Send "Do not worry your patient is good" to N
End

Fig. 3 The mechanism from doctor to storage site

IV. SIMULATION RESULTS

To simulate and evaluate network performance, we used the MATLAB 2014.

When sent from the patient to the storage site and assuming that 6 readings are done per hour, we actually enter 6 values from a patient's.

TABLE I
VALUES ENTERED FROM PATIENT

Patient temperature	**38**	**Sugar ratio**	**76**
Oxygen Saturation ratio	**90**	**Pulse per minute**	**70**
Frequency of breathing rate	**20**	**Blood pressure**	**9/12**

When this information is sent from the patient to the storage site, the used RSA values are:

P (site) = 149 , Q (site) = 173

Then P → S time required to implement the entire algorithm is 36.2145 sec, RSA time needed to implement encryption and decryption is 28.04925 sec, Pup/Pri time needed to generate public and private keys is 0.0225 sec.

When sending a patient message from the site to the doctor:

P (doctor) = 61, Q (doctor) = 53, Public(doctor) = 7.3233, Private(doctor) = 1783.3233

RSA time needed to implement encryption and decryption is 3.92775 sec, Pup/Pri time needed to generate public and private keys is 0.02 sec.

Send a response from the doctor to the site:

P (site) = 149, Q (site) = 173, Public(site) = 3.25777, Private(site) = 16971.25777

D → S time required to implement the entire algorithm is 8.7825 sec, RSA time required to implement encryption and decryption is 4.7675 sec, Pub/Pri time required to generate public and private keys is 0.02 sec.

After receiving the response to the site, decryption and knowing the patient's condition, a reassurance message is sent to N, encryption and decryption is done with the master key of N:

Master(N) = 11

The response is then sent from the site to the patient:

P (patient)= 97, Q(patient)= 173, Public(patient)= 5.16781, Private(patient) = 6605.16781

RSA time required to implement encryption and decryption is 5.36825 sec, Pub/Pri time required to generate public and private keys is 0.02 sec.

When sending readings from the patient's body, we can send 6 values to different sensors as mentioned earlier or we can send 6 different readings for the same sensor during an hour for example, monitor the patient's temperature during an hour. This gives diversity and difference in the possibility of using our network.

- By sending an ID doctor with the data we were able to include more than one doctor within the network but without knowing anyone else 's information.

- With these developments and by adopting a two-stage communication between the patient and the doctor through the storage site: if we include more than one patient in the network, we do not need to give the doctor new keys for each patient and thus we have provided the number of keys used.

Using MATLAB and introducing real values for readings from a patient's body and real values of the keys used to encrypt and decrypt, we got high performance and realistic results where the data was sent and received successfully with the security and protection of the network by using RSA encryption and decryption technology with our developments.

V. CONCLUSIONS

In this paper, we proposed a secure architecture of WBSN, in order to achieve the most important security requirements as privacy and confidentiality. The evaluation of this architecture confirmed that it is suitable for real time applications since it needs very little time to be executed.

REFERENCES

[1] Victor Shnayder, Bor-rong Chen, Konrad Lorincz, Thaddeus R. F. Fulford-Jones, *and* Matt Welsh, “Sensor Networks *for* Medical Care”, Harvard University Technical Report TR-08-05, April 2005.

[2] B. Lo and G. Z. Yang. "Key technical challenges and current implementation of body sensor networks”. IEEE Proceedings of the 2nd International Workshop on *Body Sensor Networks* (*BSN*'05), pp. *1*–5, April *2005*.

[3] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton. "Codeblue: An ad hoc sensor network infrastructure for emergency medical care”. International Workshop on Wearable and Implantable Body. *Sensor Networks*, April, London, UK *2004*.

[4] L. Zhong, M. Sinclair, and R. Bittner. "A phone-centered body sensor network platform: cost, energy efficiency and user interface". In proc. BSN 2006.

[5] R.Gnanavel, P.Anjana, K.S.Nappinnai, and N.Pavithra Sahari, “Smart Home System Using A Wireless Sensor Network For Elderly Care”, Second International Conference on Science Technology Engineering and Management (ICONSTEM), 2016.

[6] C. Karlof, N. Sastry, and D. Wagner. "Tinysec: a link layer security architecture for wireless sensor networks". In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, 2004.

[7] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. "SPINS: Security protocols for sensor networks". In Seventh Annual International Conference on Mobile Computing and Networks (*MobiCOM 2001*), pages 189–199, 2001.

[8] L. Eschenauer and V. D. Gligor. "A key-management scheme for distributed sensor networks". In Proceedings of the 9th ACM conference on Computer and communications security 2002.

[9] L. Lazos and R. Poovendran. "Serloc: Secure range-independent localization for wireless sensor networks". ACM TOSN 2005.

[10] D. Liu and P. Ning. "Establishing pairwise keys in distributed sensor networks". In First IEEE Int'l Workshop on Sensor Network Protocols and Applications, May 2003.

[11] E. Mykletun, J. Girao, and D. Westhoff. "Public key based cryptoschemes for data concealment in wireless sensor networks". IEEE International Conference on Communications. *ICC-2006*, Istanbul, Turkey, June 2006.

[12] S. Capkun, L. Buttyan, and J.-P. Hubaux. "Self-organized public-key management for mobile ad hoc networks". *IEEE Transactions on Mobile Computing*, Vol: 2 , Issue: 1 , Jan.-March, 2003.

[13] W. Du, R. Wang, and P. Ning. "An efficient scheme for authenticating public keys in sensor networks". In Proceedings of *MobiHoc*, pp58-67, 2005.

[14] M. Nemec, M. Sys, P. Svenda, D. Klinec, and V. Matyas. "The Return of Coppersmith’s Attack: Practical Factorization of Widely Used RSA Moduli". the 2017 ACM SIGSAC Conference, November 2017.