IJCAT International Journal of Computing and Technology, Volume 1, Issue 5, June 2014
ISSN : 2348 - 6090
www.IJCAT.org

Security Algorithm for Wireless Patient Monitoring System

[1] Priya S. Wagh, [2]Anagha P. Khedkar

[1] Department of Electronics &Telecommunications Engineering, Pune University, Nasik, Maharashtra, India

[2] Department of Information Technology , Pune University, Nasik, Maharashtra, India

Abstract - Hacking of Wireless network leading to insecure data is the main issue that needs to be attended. To achieve the goal of data security, there is need of the Security algorithm especially for medical applications using wireless communication. The proposed system includes Rivest Cipher 4 (RC4) security algorithms to ensure data security. Personal biomedical information can be relatively easy to be accessed due to the nature of wireless or internet based communication. Therefore there is a possibility of being abused and the personal information may be put to a bad use. Hence, it will be necessary to apply security technology through which only the server and end point user can read data correctly in the healthcare system. On the basis of a reliable scheme, the proposed work is to design and implement this novel system using ZigBee device for patient monitoring, which integrates temperature, pulse rate monitoring. The result of security algorithm implementation assures the secure network for master and slave communication.

Keywords **- Rivest Cipher 4, Zigbee**

1. Introduction

A healthcare system monitors bio-.information, personal data etc. of a patient or patients (end point) that receives medical service. This information is being transmitted to a remote healthcare server through wireless network [1]. The server can monitor health status. Physician can utilize this information and diagnose and take appropriate measures to a particular client. In an emergency accident cases, vital signs are transmitted to the remote healthcare server and a prompt clinical service can be provided with, which may save one's life. However, this personal information can be relatively easy to be accessed due to the nature of wireless communication. Therefore a possibility of being abused and the personal information may be put to a bad use [2]. Hence, it will be necessary to apply security technology through which only the server and end point user can read data correctly in the healthcare system. In this system, proposed RC 4 based encryption algorithms which is suitable for patient monitoring system and tested them successfully.

1.1 Motivation

In many wireless patient monitoring systems comprises transmission of vital sign in which hacking of Wireless network leading to insecure data is the main issue that needs to be attended. Therefore, to meet the goal of ensuring security in biomedical field in which only the server and end point user can read data correctly. Hence hacking to wireless network motivated to implement secure network.

1.2 System Objective

- To design a ZigBee based Wireless sensor network for patient monitoring
- To send vital patient information and receive using ZigBee based WSN.
- To apply security algorithm in master and slave communication

2. Proposed System Overview

Patient Monitoring System consists of network connection between master and slave communication as shown in the Fig. 1

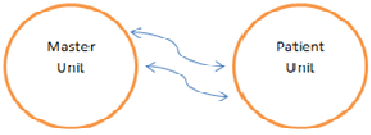
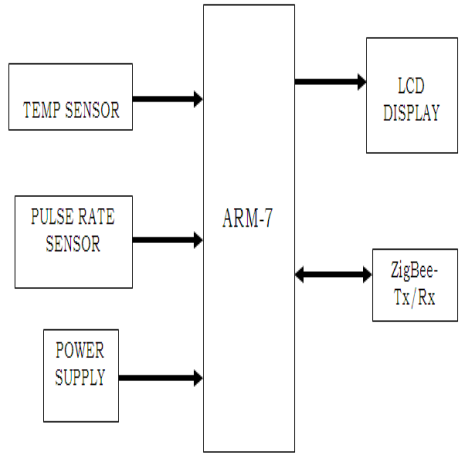
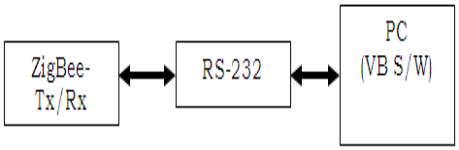


Fig-1: Network connection between Master and patient unit.

Master unit present at the doctors room or at the authorized person room PC master contain VB software on it. Master unit communicate with patient unit with the help of Zigbee based wireless network



(a) Patient Unit



(b) Master Unit

Fig -2: Block Diagram of Patient Monitoring System

Fig 2. Show block diagram for patient monitoring system. A main Server displays patient data and also monitors the status of all the patients which covers the whole area. Patient unit integrates pulse rate and temperature sensors.

2.1 Flow of Proposed System

- Initialization of S.
- Initial permutation of S
- Swapping of bit
- Stream Generation.

3. Security Algorithm

It is necessary to encrypt data transmission being transmitted at the client point to increase the strength of information security. There are various types of security algorithm such as Blowfish, data encryption standard (DES), advanced encryption standard (AES), Rivest Cipher 4 (RC4). There are two types of implementation of algorithm one is Block cipher type and Stream cipher type.

Blowfish, data encryption standard (DES), advanced encryption standard (AES) security algorithm uses Block cipher type and Rivest Cipher 4 (RC4) uses Stream cipher type for implementation of the algorithm. These types have a characteristic of simple operational process. Block cipher uses a fixed-length groups of bits called block and return cipher-text) n-bit block with respect to an n-bit of plain text block input. Stream cipher substitutes cipher text output following a pseudo-random cipher stream for plain text input.

A key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are apparently random. A pseudorandom stream is one that is generated by an algorithm but is unpredictable without knowledge of the input key. The output of the generator, called a stream of key, is combined only one byte at a time with stream of plaintext using the exclusive-OR (XOR) bitwise operation.

RC4 is a symmetric stream cipher algorithm [3]. RC4 is consists of two segments. They are permutation process of 256 Bytes and two 8-bit index pointers. The permutation is initialized by a variable length key using the key-scheduling Algorithm (KSA). Once this is completed the stream of bits is generated using the pseudo-random generation algorithm (PRGA). In this part, contain a 128-bit key. In Key Scheduling Algorithm, 256-bit Array S is filled from 0 to 255 and swap values of S with the key. PRGA changes the state and generates one-byte key stream output. In each loop, PRGA increments i and the value of S[i] is added to j. S[i] and S[j] are switched and output becomes the value of S[S[i]+S[j] mod 256]. Each element of array S is changed at least once.

4. Implementation using RC4

The RC4 algorithm is simple and quite easy. RC 4 uses two array State and Key

- 256-byte state table.

State [256] = [0 ... 255]

- It has the capability of using keys between 1and 2048 bits.

Key [1...2048] = […….]

In the implementation part contain following two phases

- Key Setup

1. $f = (f + Si + Kg) \bmod 4$

2. Swapping *Si* with *Sf*

- Ciphering (XOR)

1. $i = (i + 1) \bmod 4$, and $f = (f + Si) \bmod 4$
2. Swapping *Si* with *Sf*
3. $t = (Si + Sf) \bmod 4$

Random byte *St*

Therefore processing steps[4] involve in this type of algorithm

- Initialization of S
- Stream Generation

It will result into cipher text obtain from above process of implementation

5. Result

After Implementation of RC 4 with its steps result obtain which comprise of secure data network between master and slave communication.

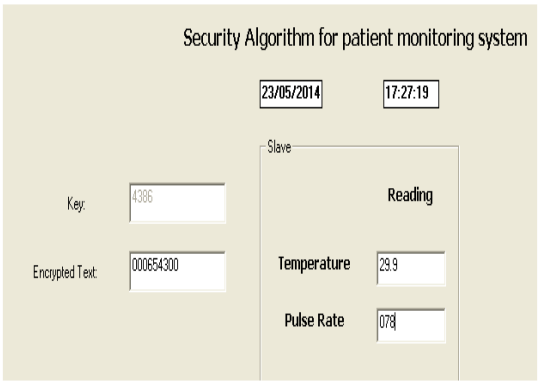


Fig -4: Result with correct entry of secure key

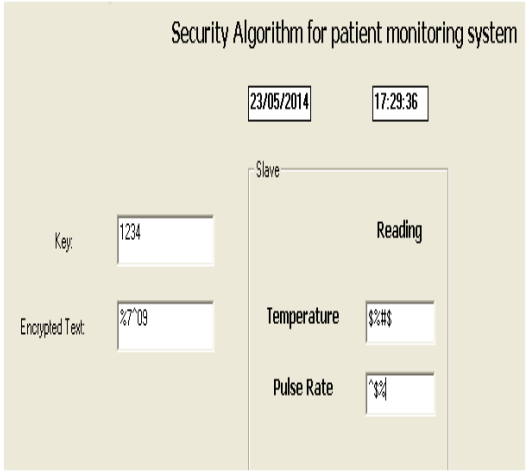


Fig -5: Result with correct entry of secure key

In this system, if authorized person enter correct secure key then only data regarding patients will be access as shown in fig. 4. If any person with unknown of the secure key he fails to access the data regarding patient as shown in the fig. 5.

6. Conclusion

It has been observed from the result that the security algorithms that were necessary to secure data transmission in a patient monitoring system. The security algorithms that work properly in an embedded system with limited computation capabilities and small memory unit. Implementation of security algorithm which secures the biomedical information for military medical services application also.

References

[1] K. Jeong, E-Y Jung, and D. K. Park, "Trend of wireless u-Health," in 9th symposium on Communications and Information Technology 2009 (ISCIT 2009), Incheon, Korea, 2009, pp. 829–833..

[2] H. S. Ng, M. L. Sim, and C. M. Tan, "Security issues of wireless sensor networks in healthcare applications," BT Technology Journal, vol. 24, no. 2, pp. 138–144, April 2006.Varshney and Sweta Sneha, "Wireless Patient Monitoring: Reliability and Power Management," 2005 IEEE.

[3] P. Prasithsangaree, and P. Krishnamurthy, "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in IEEE Global Telecommunications Conf. (GLOBECOM '03), pp. 1445–1449.

[4] Knudsen, L., et al. "Analysis Method for Alleged RC4." Proceedings, ASIACRYPT '98, 1998.