International Journal of Engineering & Technology, 7 (2.32) (2018) 331-335

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secure Quantum Key Distribution Encryption method for Efficient Data Communication in Wireless Body Area Sensor Net-works

Y. Sai Suguna[1], B. Kavya Reddy[2], V. Keerthi Durga[3], A. Roshini[4]

[,2,3,4] *Department of Computer Science and Engineering, K L E F, Vaddeswaram, Guntur Dist, AP-INDIA*
**Corresponding author E-mail: ysaisuguna@gmail.com*

Abstract

Wireless sensor networks has found its advancement in sensing the physiological parameters of human body through WBAN. Such nodes are either implanted or surface mounted on the human body in a particular position. The main purpose of these networks is to send the data generated by the wearable device outside the WLAN or the Internet. The BAN will continuously monitor the psychological changes like blood volume pressure (BVP), Brain signals etc. Uncertainty in the normal values will result in transmit all the information to the respective recipient to take required treatment. If an emergency is detected, the doctor instantly updates the patient's health by sending a specific message. There is limited confidentiality, so the intruders will gather sensitive data. Public key cryptography can be used to create an unprotected communication channel. It also provides a convenient way to implement keys. This paper is focusing on a unique key generation technique called Quantum key distribution, which is used to create symmetric key method by using quantum properties of optics to transfer information from one Client to another in One-Time Pad manner. The special feature of the technique is to guarantee that the key cannot be intercepted during transmission without alerting the users to provide high authentication for received data.

Keywords: *Wireless Body Area Networks (WBAN), Message Authentication Code (MAC), Quantum key distribution, Base Server (BS), BAN Nodes (BNs).*

1. Introduction

Wireless Sensor Networks are often represented as a set of sensing element called nodes, which were able to sense the environment interaction between individuals and computers and even the encompassing surroundings.[10] Wireless Body Area Networks consists of in-body and on-body sensor nodes that endlessly monitor patient's sensitive information for diagnosing and prescription. Some on-body nodes are used for transmission and gaming applications.[11] Wireless Sensor Networks consists of many multi-functional sensing nodes densely arranged in a very massive region controlled by base station and are connected to the web or alternative networks to the wireless sensor networks. [14] Every sensor node consists of a radio frequency transceiver, a central processing unit for processing the data, a power supply like batteries and memory for storing data. Such sensors are used to sense physical parameters like temperature, light, pressure, vibration, humidity, sound, radiation. [16] All of these sensor nodes acquire information, process the information and route the information to the sink node. Since the sensors are collecting user's personal medical information, privacy security and are vital elements in a body sensor network.[17] At the same time, the collected information should be promptly accessible at the time of an emergency. But the present available data storing and accessing approaches in Wireless Sensor Networks are divided into 2 branches they are centralized approach and distributed approach.

In the case of centralized approach, detected data is collected from individual's sensors and is sent back to a central location, usually the sink, for accessing and storing purpose.

In the distributed approach, when a sensor node has generated some information, it stores the information regionally or at some selected nodes inside the network rather than instantly forwarding the information to a centralized location out of the network.[13] Then, the data is stored should be distributed to them in the logged-in Wireless Sensor Network can be accessed as well.
When compared to the centralized case and distributed information, both storing of data and accessing of data consumes less bandwidth since sensed data are no longer transmitted to a centralized location out of the network.[2] In wireless networks, the transfer of information is a broadcast service where the information is distributed to all possible directions in the medium within a restricted range. Wireless networks do not promise quality of service during transmission and possibilities of intrusion into such networks are terribly high since the transmission here takes place through the medium of air and not cables. So as to form secure communications around Wireless Sensor Networks, communication between the sensor nodes and base station to sensor node ought to be handled carefully.

2. Literature Survey

Cryptography is a method of data communication in a secure way at the presence of third parties, known as hacking person or the intruder. [1]Classical cryptography relies on the complexness of some mathematical functions that could be a single way function. The safety of the sensitive data is very good, also it could not be taken.[5] It provides security, the only weakness of classical cryptography is that it doesn’t serve any methodology to sender and receiver to watch out for the existence of any intruder around it. And the typically used classical cryptographic technique is RSA that depends on problem of factorization of numbers that are obtained by product of 2 giant primes. Wireless Body area sensor networks have the full form of lightweight Identity-Based Encryption. Privacy & balanced secure can be achieved by protocols with the help of accessibility.[3] Here, Security keys count of ‘n’ released by our proposed scheme. For generating the n+ 1 key, the master key can be accessible. We have a typical of novel in BSN, communication of inter sensor security which is also known as Physiological Value based Security. this can be simply called as PVS. By keep secreting the values of physiological, this system allotted a key with a message. Our system is in use if the whole sensors observes and measures signals of single IPI which are like values of Physiology that are much difficult. [6] These are accurate for removing a complete distribution of keys. In 2011 another typical system came into exist. With help of BSN, the patient can be monitored who is in home in this system. This is helpful for the senior citizen patients who want continuous monitoring at home. As this not used the security which is end to end, it not considerable.[5] Again in 2011, another technique came into existence which is like Wireless Body Network Attacks In this data can be sent and receive using Wireless Body Area Networks i.e wireless sensors from specific or authorised to registered sources. For overcoming the attacks, it used the digital certificates. In 2009, a scheme of Wireless Body Networks distributed key management came. Here, at first the server and nodes of servers are preloaded with some keys. If initial key is agreed then remaining keys are wasted.

3. State of Art

Because quantum system is useful for all types of classical cryptosystems, but it has these missing shortcomings in the classic cryptosystem in mind, individuals began to assume outside the range of it for securing future transmission. Quantum cryptography can find solutions for almost all of the flaws found in classical cryptosystem.[19] For the first time in cryptography, quantum mechanical forces are used to obtain a secure unconditional cryptography system. In the initial part we discuss regarding secure key management technique, second next part includes the discussion regarding the quantum cryptography, and in last part, we implement the quantum cryptography in wireless local area network.

4. Quantum Key Distribution Encryption

4.1 Secure Key Management Technique

The proposed & implemented system is the Wireless Body Area Network mechanism for secure key management. It having the Wireless Body Area Networks set which is connecting to server of backend.[7] With the help of internet, the sensor measured information of biometric from node of the sensor to the server of master with the relay of Backend server. Based on a id of a node every sensor find out the server of the master.[19] A secret key which is unique can be generated master server for every node of the sensor. If a node want to go for a network then that node send request to master server which is protected with MAC through server of backend.[5] The MAC can be verified by master server provides message& master key to that node and again it transmitted to the backend server. The key belongs of the message & master can be encrypted by backend server and transmitted the particular node of the sensor for starting the process of the joining. After completion of receiving the keys by all nodes, the rekeying time can be scheduled by BS for refreshing the master key.

4.2 The Proposed Architecture

Wireless Body Area Networks set that consists of, Server of Backend (BS) & Server of Master (MS).

Figure 1 describes a network of Wireless Body Area Network having a sensor that is deployed in human body. All these are having the communication with Backend Server.[15] Wireless Body Area Networks connected to the Backend Server are having a communication network with the Master Server.

a. Message Key (Kmsg)

It is used for providing communication between backend server & nodes of all sensors.

b. Master Key (Kmas)

With help of rekeying scheduling, its refresh message key.

c. Secret key (Ksec)

Security key is unique key. it can be sharable to master server. Each is node having a separate security key.

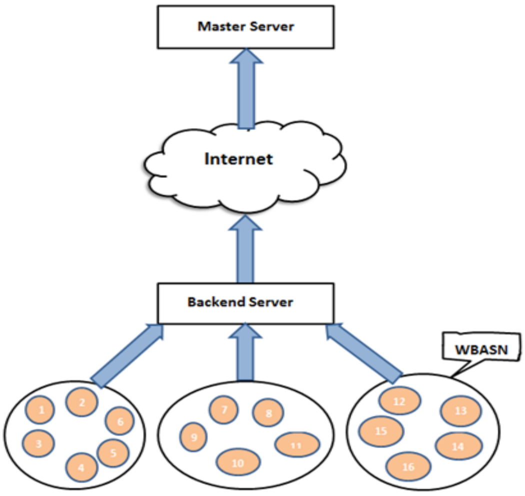
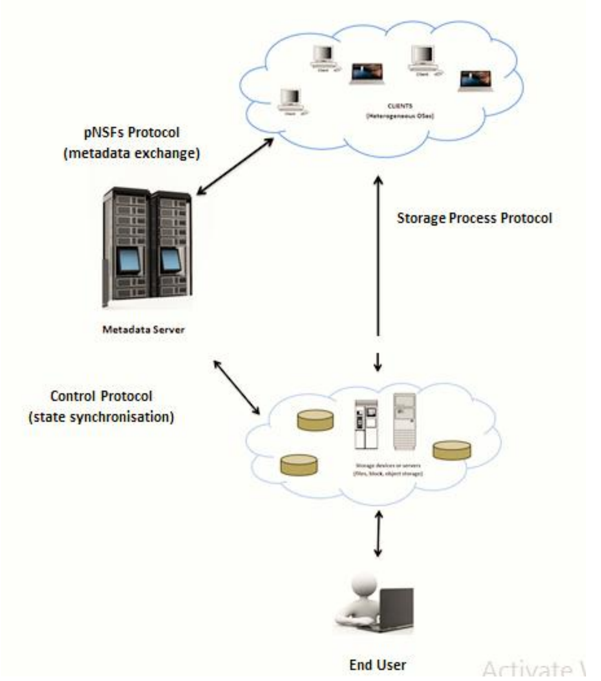


Fig.1. System Architecture

4.3 Storage Server Architecture

A storage server will process the data and stores the data in storage devices or servers. A streaming server deployment requires at least one metadata server (the primary storage server). All the data is saved in storage devices or servers (files, blocks, object storage) or folders, is presented to both the system storing it and the system retrieving it in the same format. Install the metadata server before installing any normal servers. File storage architecture is also called as file-based storage architecture, which stores data in a metadata server. Data can be accessed using the Network File System (NFS) protocol. Parallel Network File System (pNFS) is part of the Network File System that allows all the clients to access storage devices directly. This is achieved by separating data and metadata and moving the metadata server out of the data path.



.

Fig.2. Storage Server Architecture

4.3.1. Manual Authentication Technique

For transmitting the manual data among the all devices, it uses the wireless devices & wireless channel authentication. [9] Reproduction of output data to one appliance to another device, Two devices output comparison; enter same information in both device can be done in transfer of data manually.[8] Here no need of entering the data by user. Usually, the person has to enter 32 binary digits.

4.4 Implementation of Quantum Key Cryptography

1. The encryption & authentication is necessary for every transmitted message in network.[18] The symmetric key shared with SensorNodes and Master Server is given by

$SNi\ K\ k\ (SN\ )sy\ sec\ i = \lambda$ -- ----(1)

λ is function of pseudo random.
Ksec (SNi) = secret key.

SNi - the server of master sent a master key to each node which is unique after authentication Successful.

2.Two sub keys holed by Ksec, those are key for encryption key (ke) & key for Message Authentication Code.

(kmac): $K\ k\ K\ M\ e\ mac = +$ --- (2)

$Ksec\ SN\ MS\ i \leftarrow$ (3)

3. If the a data transmitted from Sensor node to Master server, then it can be encrypted with the help of ke & signed; by using MAC key Kmac - before transmission. Format for this is
$SN\ MS\ :\{d\ |\ t\ \}\ mac(K\ \{d\ |\ t\ \}\ )\ i\ s\ ke,$

$mac\ \ s\ ke \rightarrow$ *(4)*

I. data represented as D
II. Time stamp while the data transmission done represent as Ts
III. mac (K, d) for message computation authentication code
IV. Message - d with key K.

If any node data received by Master Server. it verifies data and then decrypted. With the help of Key of encryption and MAC, a secure connection can be established.

4.4.1. Initialization

For joining into a network, with the help of Master Server,[18] The nodes of each sensor has been initialized. Here, sharing of symmetric key done between Master Server& Backend Server. By using the private & channel of out band all this process can be done. Depending on the nodes of sensor physical characteristics, Authenticate & private channel creation can be done.[12] Confidently we can transmit the data via channel, integrity of data & authentication are all obtained in this method. Here, the gateway function done by backup server. The communication in between nodes of WBNS & server of master activates the node of Sensor SNi securely in this private channel. Out-of-band channel transferring of data involves the following steps.

1. Master server receives the ID of SNi from Sensor node – ID

$SN\ MS\ i \rightarrow$ ------------ - (5)

2. In explicit nature, this can be done. Because of special properties of Out of band channel, SNi ID can be done implicitly.
3. The Secret key which is randomly generated by Master server send to the

$SNi\ \ \text{-}Ksec\ SN\ MS\ i \leftarrow$-------- (6)

Ksec stores in Sensor node as well as in Master server of memories. So we can say that the each nose of Sensor SNi having a separate KSec Secrete key. And it also having a unique Counter (C) which have the 0 initial values i.e (CTR→0) is in buffers of sensor.. To prevent attacks reply & consistency guarantee, counter values are helpful. [20] Every time the value of the counter increased by one after accessing it.

4.4.2. Joining of Nodes

In the below prospects, network added the new nodes, to monitor Biometrics, New nodes development done, Node device Malfunctioning, below algorithm describes the joining of nodes procedure:

4.4.3. A join request (JREQ) forwarded by Sensor Node i to Base station

1. Sensor Node sends a join request to the Base Station.

$JREQ\ SN\ BS\ i \leftarrow$ *(7)*

2. With help of Ksec generated by MAC while SNi Joining, The protection of JREQ done -sec JREQ : MAC _ K BS sends

$JREQ\ to\ MS\text{:}\ JREQ\ BS\ MS \rightarrow MS$ (8)

Verification of the MAC and message key Kmsg generated initially and Node of master key Kmas sending to

$BS\ \text{-}\ MS\ BS\ K\ K\ msg\ mas\ + \rightarrow BS$ - (9)

Kmsg with Kmas encrypts & forward to the Sensor Node

$EK\ \{K\ \}\ mas\ msg\ BS\ SN \rightarrow i$ (10)

4.5 One-Time Pad Manner

A One-time pad is a symmetrical cryptosystem that is a form of cryptosystem that has been verified as indestructible even if it is forced to apply. Each character or bit of the plaintext is encrypted with a standard addition of a character or bit of a secret random key (or pad) of a similar length as the plaintext, changing it into a cipher text. OTP cannot be unbreakable if any of the following conditions is endangered.[4] If key information of Master Server received by SNi, The time period of rekeying done for refreshing the key of the msaster server. The rekeying period can be broadcasted by BS with Kmsg which is newly updated, encrypting done with Kmas to Nodes of sensors SNi - EK {K } mas msg BS SN → i rekeying request (RE_REQ) can be send by Sensor Node i, in the period of rekeying request (RE_REQ) send via Backend Server to the Master Server - RE _ REQ i RE _ REQ SN BS (Authentication channel) MS → → MS updated the master key K'mas which is newly generated sends to K'mas that can be encrypted with Ksec for All Sni respectvely :

Ek ' mas{K } msg MS SN → i ------- (11)

5. Proposed Algorithm:

1st Step: WBANs set,; Server of Master; server of Backend; included in proposed architecture is .network of WBN having the some sensors consists of few sensor devices deployed on a human body which are connected to a Backend Server (BS)

Step 2: The Server of backend server and master having a shared symmetric key. All nodes of the sensors find outs the sever of the master the master server with the help of a node id, after that Ksec generated for each node by Master server

Step 3: if a node wish to enter into a network, it requested the master server by sending the REQ. Message Authentication Code protect the REQ with the help of secret key of ksec for node joining

Step 4: After getting the Message of request, it can be transferred from back end server to master server.

Step 5: MAC can be verified by master server initial message key kmsg can be generated by master key kmas for each node transferred to backend server

Step 6: kmsg encryption with kmas did with backend server. Transmitted to sensor nodes

Step 7: After whole nodes receiving the information of key from server of master server, & BS scheduled rekeying time for refreshing master key

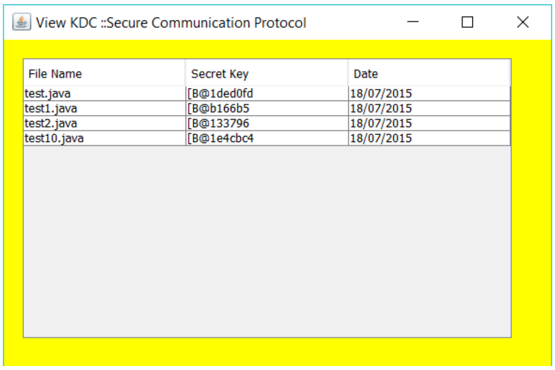
6. Results

6.1. Simulation Parameters

The NetBeans IDE 8.1 is utilized for simulating the proposed Secure Key Management Technique.

6.2. Implementation

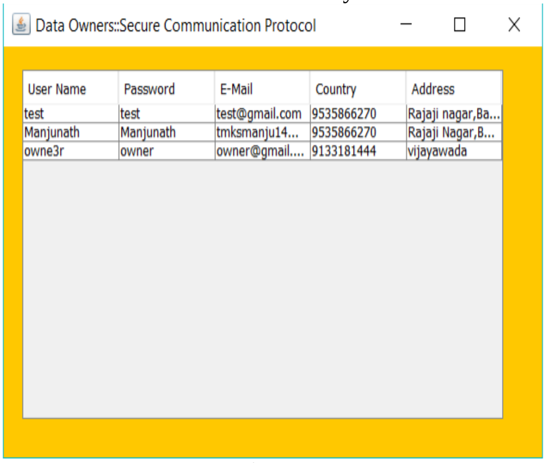
According to the *QUANTUM KEY DISTRIBUTION PROTOCOL* a high quality pseudo random number is generated and distributed as a secret key.



File Name	Secret Key	Date
test.java	[B@1ded0fd	18/07/2015
test1.java	[B@b166b5	18/07/2015
test2.java	[B@133796	18/07/2015
test10.java	[B@1e4cbc4	18/07/2015

Fig.3. Quantum Key Distribution Protocol

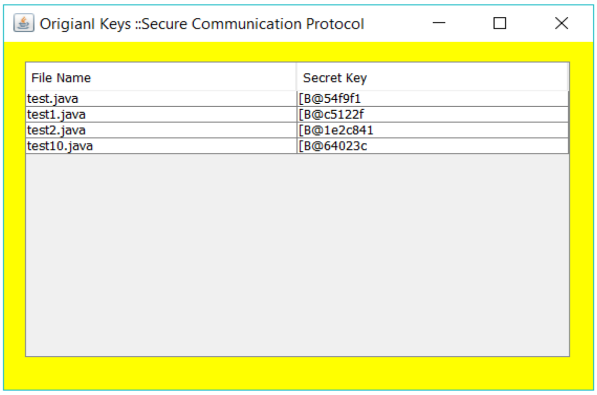
All the data that is collected during registration process of the *DATA OWNER* is stored successfully.



User Name	Password	E-Mail	Country	Address
test	test	test@gmail.com	9535866270	Rajaji nagar,Ba...
Manjunath	Manjunath	tmksmanju14...	9535866270	Rajaji Nagar,B...
owne3r	owner	owner@gmail....	9133181444	vijayawada

Fig.4. Data Owner

The symmetric key that is generated first is shared with Sensor Nodes and Master Server. Message Key (Kmsg) is for providing a communication between backend server & nodes of all sensors. Master Key (Kmas) is with help of rekeying scheduling, it will refresh message key.Secret key (Ksec) or Security key is unique key. it can be sharable to master server. Each node having a separate security key.



File Name	Secret Key
test.java	[B@54f9f1
test1.java	[B@c5122f
test2.java	[B@1e2c841
test10.java	[B@64023c

Fig.5. Original keys

7. Conclusion

Wireless Body Area Network Secure key management method proposed in this study is interfaced to the server of the backend in the implemented architecture. By using the internet, sensors node measure data of the biometric that is sent to a server which acts as master by Backend server.[20] Based on Quantum Key Cryptography, data is security is maintained on the sensitive data during transmission with the help of quantum mechanics where photons are used for communicating with other location. Due to the usage of light medium for transmission of key through One Time Pad Manner, the results obtained in simulation in proposed work depict considerable packet delivery ratio, less overhead & delay and highly secured data with no loss.

References

[1] William Stallings, “Cryptography and network security design and principles”, Pearson Education, 2008.

[2] R.Lalu Naik, Dr.P.Chenna Reddy, U.Sathish Kumar, Dr.Y.V.Narayana, “Provely Secure Quantum Key distribution protocol in 802.11 Wireless Networks”, International Journal of Computer Science and Information Technologies, Vol. 2 (6), PP.2811-2815, 2011.

[3] Hybrid unified-slot access protocol for wireless body area networks. Int. J. Wireless Inform. Networks, 17: 150-161. DOI: 10.1007/s10776- 010- 0120-2 Mohanavalli, S.S. and S. Anand, 2011.

[4] Preventing impersonation attacks using digital certificates in WBAN. Int. J. Adv. Engin. Sci. Technol., 9: 31-35. Shelby, Z. and C. Bormann, 2011.

[5] A study of MAC protocols for WBANs. Rev. Literature Arts Am., 10: 128-145. DOI:10.3390/s10010012,Venkatasubramanian, K.K. and S.K.S. Gupta, 2010.

[6] KeyRev: An efficient key revocation scheme for wireless sensor networks. IEEE International Conference on Communications, Jun. 24-28, IEEE Xplore Press, Glasgow, pp: 1260-1265. DOI: 10.1109/ICC.2007.213 Zimmerman, T.G., 1996.

[7] Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma, “Implementation of Quantum Key Distribution in Wi-Fi (IEEE 802.11) Wireless Networks”, ISBN 978- 89-5519-136-3 ICACT, PP.17-20, Feb 2008.

[8] IBELite: A light weight identity based cryptography for wireless body area networks. IEEE Trans. Inform. Technol. Biomed., 13: 926-932. DOI: 10.1109/TITB.2009.2033055 Ullah, S., B. Shen, S.M.R. Islam, P. Khanemail and S. Saleem et al., 2009.

[9] Gehrmann, C., C.J. Mitchell and K. Nyberg, 2004.Manual authentication for wireless devices.Cryptobytes, 7: 29-37.Khan, P., M.A. Hussain and K.S. Kwak, 2009.

[10] Medical applications of wireless body area networks. Int. J.Digital Content Technol. Appli.,Li, C., J. Li, B. Zhen, H.B. Li and R. Kohno, 2010.

[11] Security architecture for at-home medical care using body sensor network. Int. J. Ad-hoc, Sensor, Ubiquitous Comput., 2: 60-69.Nabi, M., T. Basten, M. Geilen, M. Blagojevic and T.Hendriks, 2010.

[12] A Robust Protocol Stack for Multihop Wireless Body Area Networks with Transmit Power Adaptation. In 5th International Conference on Body Area Networks, (BAN’ 10), ACM Press,New York, USA, pp: 77-83. DOI:10.1145/2221924.2221941Raazi, S.M.K.U.R. and H. Lee, 2009.

[13] BARI: ADistributed Key Management Approach for WirelessBody Area Networks. IEEE InternationalConference on Computational Intelligence andSecurity, Dec. 11-14, IEEE Xplore Press, Beijing,pp: 324-329. DOI: 10.1109/CIS.2009.186Saleem, S., S. Ullah and H.S. Yoo, 2009.

[14] On the SecurityIssues in Wireless Body Area Networks. Int. J.JDCTA, 3: 178-184. DOI:10.4156/jdcta.vol3.issue3.2Saleem, S., S. Ullah and K.S. Kwak, 2011.

[15] A study ofIEEE 802.15.4 security frame work for wirelessbody area networks. Sensors, 11: 1383-1395. Sharma, N. and E.M. Bansal, 2011.

[16] 6LoWPAN: The Wireless Embedded Internet. 2nd Edn., John Wileyand Son , ISBN-10: 1119965349, pp: 244.Singelee, D. and B. Preneel, 2007.

[17] A secure low delay protocol for multihop wireless body area network. Ad Hoc Sensor 8 Wireless Netw., 9: 953-72. Tan, C.C., H. Wang, S. Zhong, Q. Li, 2009.

[18] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring", *Proc. 35th Annu. Symp. Found. Comput. Sci.*, pp. 124-134, Nov. 1994.

[19] M. Blum and S. Micali, “How to Generate Cryptographically Strong Sequences of Pseudo Random Bits”, 23rd IEEE-FOCS, 112–117 (1982).

[20] Halder, M., Beveratos, A., Gisin, N., Scarani, V., Simon, C., Zbinden, H.: Entangling independent photons by time measurement. Nature Physics 3, 659–692 (2007).