Energy Efficient and Security Based Data Communication in Wireless Body Sensor Networks

A. Siva Sangari[1] and J. Martin Leo Manickam[2]

[1]Department of Information Technology, Sathyabama University, Chennai, India.
[2]Department of ECE, St. Joseph College of Engineering, Chennai, India.

(Received: 30 January 2015; accepted: 06 March 2015)

An emerging research in today is based on monitoring physiological information of human being at any place and any time using advanced technology of Wireless Body Sensor Network (WBSN). The most challenging problems in WBSN is securing and increasing the transmission performance of data in a wireless communication network. To increase the security and reliable transmission of data in WBSN, this paper proposes a light weight cryptographic HIGHT(High Security and Light Weight) technique combines with ECG (electrocardiogram) signal based establishment of key for secure communication in Wireless Body Sensor Network (WSBN). For a reliable transmission of data, utilize the clustering technique between patient's body sensors to a nearby base station. In this technique, body aggregator connects with all peripheral nodes, which allows simplified routing in network and improve high data throughput in Body Sensor Network (BSN).

Key words: Wireless Body Sensor Network (WSBN),
Hybrid Authentication Protocol, Electrocardiogram (ECG).

The facility to continuously monitor a human's health is imperative in emergency situations, for example, monitoring in disaster and distinct diseases. A wearable device is used which is being equipped for "monitoring/sensing" the patient's health record and handle the sensed signals through communication (transmit and receive) with different Wireless Body Sensor Network (WSBN)[1]. The wireless sensor technology has developed to an extent height with a functioning rule of ubiquitous and pervasive computing. The sensors could be interconnected to structure a Wireless Sensor Network (WSN), composed of various biomedical sensor node and multi-hop networking competence that might be conveyed for long term with continuously monitor the patient's health. The communication is attained through intermediate nodes, which relay information to set up a communication channel across the nodes[2]. Subsequently, secure, scalable and energy efficient communication of patients health records, particularly their transmission of data over the wireless connection having serious security issues. The lack of sufficient security may not just lead to break the privacy of patient; additionally permit adversaries to change real data resulting in wrong treatment and diagnosis. In Wireless Body sensor Network (WBSN) short duration of the battery sensors is used and these sensors also having probability of damaged nodes. In such scenarios, sensors are constrained with memory, energy, and communication and processing capacity. Accordingly, it is clear that concentrated energy aware routing protocol is needed to offer high scalability in order that life

* To whom all correspondence should be addressed.
E-mail: sivasangariphd@gmail.com

time of network is protected acceptably high in such harsh situation.

In this paper, we achieved an energy efficient transmission by utilizing a clustering technique and proposed a light weight cryptographic HIGHT technique combines with ECG (electrocardiogram) signal based establishment of key for secure communication in Wireless Body Sensor Network (WSBN). Basically, batching sensor nodes into cluster head (CH) has been broadly acquired by the researchers to fulfil the scalability and achieve maximum energy efficiency in large WSN[3]. The idea of our proposed system is clearly illustrated in fig 1.

The bio-medical sensor devices in patient's body detect the abnormal conditions and send the sensed information to nearby base station. For an efficient and reliable transmission of data form sensor device to base station is achieved based on clustering technique. The biosensor node regularly transmit their data to nearby corresponding cluster nodes. To maintain the energy consumption among all the nodes in network is to periodically re-chosen new cluster nodes. The initial steps involves that cluster nodes aggregate the data and transmit them to the base station either directly or through the intermediate communication with other cluster nodes. A data has to be authenticated and encrypted before transmit them to the base station(BS) . The encryption process takes place using HIGHT encryption algorithm, which is suitable for low-resource device[4]. In this lightweight cryptographic algorithm unique cryptographic key is generated based on the ECG time series, these change significantly from person to person and ECG signals are extremely difficult to duplicate. In this system, the fake node registration is avoided by register the aggregated node with base station before the data transmissions[5].

The paper is organized as follows: Section II presents the related work; Section III presents the system model includes as clustering the nodes, encryption and decryption using lightweight cryptographic algorithm and Key generation; Section IV presents evaluation results based on reliable transmission and security analysis; finally, Section V presents the future work and concludes the paper.

Related work

In Wireless Sensor Network (WBSN) discussions of energy has been widely examined. A recent analysis in energy field gave us numerous different results; Reduction of data is one of successful method to accomplish maximum energy data procurement. The fundamental idea of data reduction method is to minimize the quantity of data transmitted over the network such that the energy consumption for data transmission is minimized gradually. Since transmissions are usually the most cost effective operation regarding energy utilization, reduction of data could essentially delay the lifetime of WSN's[6]. To reduce the power consumption many of researcher in the recent years explored clustering in Wireless Sensor Network. The first clustering algorithm was proposed by LEACH to minimize utilization of power. In LEACH, the clustering function is changed between the nodes, depends on duration. Transmission is used by every cluster head to forward the information to the Base Station (BS)[7]. All these techniques attempt to drag out the network performance and lifetime and to adjust the load between the nodes in WSN by utilizing some support and metrics.

Tassos Dimitriou *et al.*,[2] categorized security issues as insider and outsider attacks in Wireless Sensor Network. The intruder nodes are outsider attack and they are unauthorized participants in WSN. To prevent from attackers and attain special access to data, authentication and encryption techniques are required which might then be investigated to run across sensor network. The passive attacks such as passive eavesdropping, denial of service attacks and replay attacks are the type attacks which can only be used by intruder node. The most dangerous issue from a security perspective is an insider attack, where a challenger capturing a node and analyse its memory, can acquire its node messages and key material. Having rights to authentic keys, the insider attacker can dispatch a various kind of attacks without effortlessly being recognized such as Reporting selectively, alterations in patients' health data, intruders access to patients health data and wrong data injection[2].

Law *et al.*,[4] present a standard cryptographic technique for WSN. They review efficient energy consumptions, security properties, storage and power consumption of a various encryption algorithms, the outcome of analysis and review gives us paradigm of selecting suitable cryptographic technique for WSNs. Security is most important in an such environment, since every sensor nodes store numerous keying material to create pair wise key after implementation, memory efficient cryptographic technique are needed[4]. In an environment where accessibility of network is essential, since each sensor node that utilization up battery is no more accessible in network, efficient energy cryptographic techniques must be used.

The PSKA scheme proposed in[7] to lock the key value in vault of sender side and unlock the key value in vault by using features of physiological signal at receiver side. It is based on physiological values between the sensor nodes. PSKA allows neighbouring nodes to share the key values generated from the physiological signal. The pre deployment of keys are not needed. The addition extra chaff points will lead to unnecessary communication overhead.

The feature of physiological signal is performed by using the DWT. The feature vectors are concatenated and quantized into digital form[8]. The concatenated blocks are encrypted by SHA algorithm. The fingerprint value is used as seed value for random generator. The random generated values are used as locations for water marking image. The receiver side also fingerprint is used as seed for random generators. The message authentication code is used for integrity of input data.

In this scheme[10] before the sensor deployment ,the sensor nodes are progrmmed with then timing sequence. This sequence only specify the interval for key update. The secret key value is computed for every interval. This secret key value is sent along with encrypted data. The sender side send the encrypted data and MAC value and commitment of session key. The receiver side performs decommitement of session key and decrypt the data. Both sensors using same biometric features to commit and decommit the encryption key. It eliminates computation and communication overhead.

In Guassian model[11], the ECG signal features derived from human body are uniquely different from person to person. The IPI values are extracted from the ECG signal. The grouping of IPI values will act as key for this scheme. The IPI values from the sender are combined with medical data. The signature is created and attached to the medical information. The receiver side extracts the IPI values from ECG signal and signature is compared with the receiving signature. The stochastic pattern recognition is applied for security. It can remove the computation overhead by eliminating the key exchange process. The verification process is based on signature. This approach has tolerance against the sample alignment.

System model

The motivation of this paper is to attain an efficient and highly secure communication in Wireless Sensor Networks (WSN). In Body Sensor Networks (BSN) sensors are placed in the human body to monitor health conditions. The body sensors devices are normally controlled by an electrical energy, a most challenging issue is how to extend the lifetime of all sensor devices in BSN. For an energy efficient and reliable communication, the proposed system model specifies clustering concept to minimize the utilization of energy in data transmission and guarantee authentication and security between (i) Sensor Node's (SNs) to Sensor Head (SHs) (ii) SH to Base Station(BS) and (iii) Base Station (BS) to Medical Server managed by the hospital or medical centre.

Clustering formation in WBSN

The clustering technique in the proposed model could concentrate on the energy efficient and authenticated data transmission. The authentication process takes place between sensor node, aggregation node (sensor head), base station and medical server. The Sensor heads are grouped into clusters and individual sensors sense data and transmit to SH. Sensor heads aggregate data from different sensor nodes and then forward to the base station by using efficient protocol. In the Hybrid protocol, each SH is assumed to be a network connector that controls several sensor nodes and also utilize a distribute clustering technique so that SH takes an independent decision without having centralized management. The clustering are deployed manually depending on the location and communication range between sensor head and base stations.

The SH actually act as gateway across the sensor nodes and the BS. The activity of an every sensor head is to perform normal operations for all the nodes in the cluster, such as aggregate the information before sending it to the base station. Somehow, the SH sink for the SNs, and the BS is the sink for the SH. Also, this arrangement are structured across the sensor nodes, the SH and the BS might be replicated the same number of times as it is required. The clustering reduces the data to be transmitted to the base station by processing all data locally. When the Sensor head collects overall data and transmits it to the base station, the energy spent is reduced.

Methods for secure data transmission and authentication

This work concentrates on three stages of data transmission and they are data transmission between biosensors and sensor head, data transmission between the sensor head and the base station and data transmission between the base station and the physician. A short summary of every stage is presented below.

Data Transmission between Biosensors and Sensor Head

The main process is generating the master key from the ECG signal. The generated key also acts as session key for authentication purpose. A grouping of 128 bits can be produced from 67 IPI(Inter Pulse Interval)sequences acquired from an ECG signal .The elliptic curve cryptography is applied in feature value. multiple IPIs are concatenated together to form a secret key X. Then the sender encrypt the message using public key and receiver decrypt the data using secret key

Table 1. Notations used in this Paper

Symbol	Definition
S_{id}	Sensor node's ID
BS_{id}	Base Station's ID
M	Message
BS_y,BS_x	Base Station's Public Key and Private key
N1,N2	Nonce values
F(x)	Polynomial Form
X	Secret Key

Data Transmission between the Sensor Head and the Base Station

Each SH aggregates data from the local sensors and send the head node id to the base station. The node id is encrypted with base station's public key. The base station decrypts the node id value and verifies the id with list of node ids is stored in the base station.The sensor head send the session key is encrypted with the base station public key (BS_y) and the information of data is sent to the base station authentication is performed.

Data Transmission between the Base Station and the Remote Server

HIGHT cryptographic algorithm is used to ensure the secure transmission and ECG signals are utilized for Master keys .The physician can gain access to the data, only after providing the user name and password.

Transmission Between The Sensors

The cryptographic keys need a randomness, and keys got from irregular time changing signals have higher security, since an intruder can't dependably anticipate the genuine key. From a cryptographic point of view, symmetric encryption is suitable for the ECG-produced parallel grouping. The communication between the sensors is shown in Fig 3. The IPI is the time interval between the inter-beat (RR) peaks in the

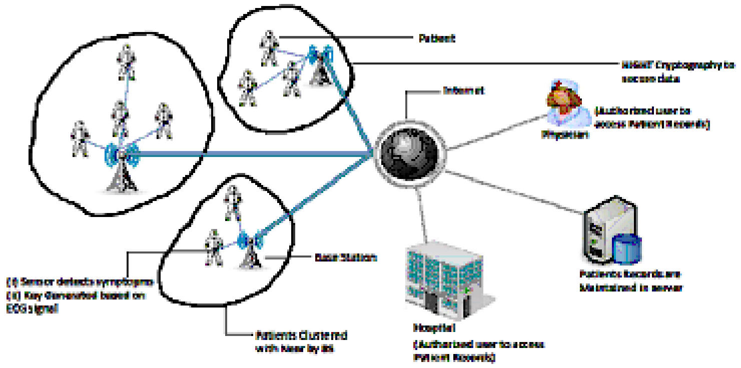
Patient
HIGHT Cryptography to access data
Internet
(Authorized user to access Patient Records)
Physician
Base Station
(i) Sensor detects symptoms
(ii) Key Generated based on ECG signal
Patients Clustered with Near by BS
Hospital
(Authorized user to access Patient Records)
Patients Records are Maintained in server

Fig 1. Basic architecture of system model

ECG signal. The main process is generating the master key from the ECG signal. The generated key also acts as session key for authentication purpose. A grouping of 128 bits can be produced from 67 IPI sequences acquired from an ECG signal inspected at 1000 Hz, and for every 128-bits succession caught at a specific time moment, sensors inside the WBSN have Hamming distance of 22 bits. If it is approximately greater than 80 bits then it does not belong to the same WBASN and it is discarded.

The purpose of proposed scheme is secure the inter sensor communication from the ECG kry generation for enabling two sensors to agree on ECC based on ECG signals generated at the different sensors.

(1) First both sensors simultaneously collect and process the ECG signal. Our proposed scheme is based on IPI method. Because it is less computational power compared to FFT. The IPI have high level of randomness. The sender and receiver collect IPI simultaneously.

(2) Once the feature value is generated. Then it is substituted in the polynomial of the form

$$F(x) = x^m + f_{m-1}x^{m-1} \ldots + f_2 x^2 + f_x x + f_0 \qquad \ldots(1)$$

Each polynomial f(x) defines a polynomial representation of $F_2^{\ m}$. The $F_2^{\ m}$ is called finite field in ECC. The order of the polynomial is known to all sensor nodes. The coefficients are generated using random generator.

(3)With the polynomial and feature vectors, now the sender calculates the points in finite field. To set up an ECC, we need to derive the secret key value. Each IPI is quantified in to 4 bits and multiple IPIs are concatenated together to form a secret key x. We generated secret key x and corresponding public key Y=X.G. The base point is G eE (F_m) .E is elliptic curve over the finite field.

Table 2. Comparison of RC5 and HIGHT techniques

Algorithm	Power Consumption (CPU cycle)	Operation Time (sec)	Memory Status	Drawbacks
RC5	70,800	7.252	72 RAM and 3,188 ROM	Key schedule is more complex, Speed optimized method
Proposed HIGHT	64,450	7.317	584 RAM and 3,906 ROM	Simple operations, Speed and size-optimized method

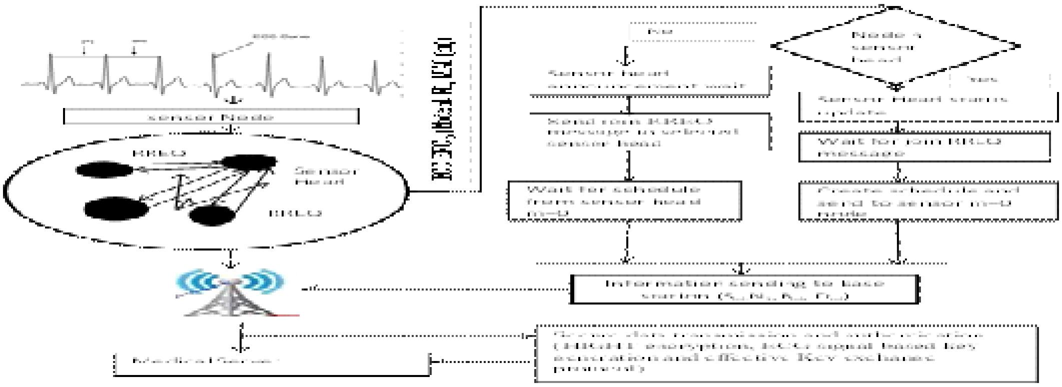
Sensor Node
RREQ
Sensor Head
RREQ
No
Yes
Send join RREQ message to selected sensor head
Wait for schedule from sensor head
Wait for join RREQ message
Create schedule and send to sensor node
Information sending to base station
Medical Server

Fig 2. Process of clustering formation

(4) Both sender side and receiver side the same operations can be performed. Then the sender encrypt the message using public key and receiver decrypt the data using secret key.

(5) The sender communicates to the receiver using the following message :

$$\text{ECC ENC}_y\ (S_{id}, N1, MAC\ (M)) \qquad \text{...(2)}$$

Node ID-Node ID uniquely identifying the sensor, N1-Nonce value for preventing replay attack, MAC (m) - Message authentication code value of message, Y-Public key.

(6)The receiver decrypts the data using the secret key value calculated from multiple IPIs. It verifies the MAC value to authenticate the sender to the receiver and nonce value is used for avoiding the replay attack.

$$ECC\ DEC_x\ (S_{id}, N2, MAC\ (M')) \qquad \text{...(3)}$$

Transmission Between The Sensor Head To Base Station

The sensor head aggregates all the information and has to register with base station before sending the data to the base station. The

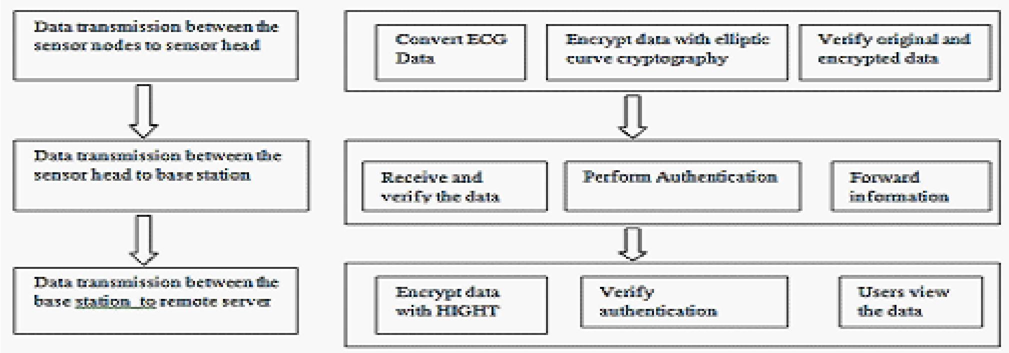
Data transmission between the sensor nodes to sensor head
Data transmission between the sensor head to base station
Data transmission between the base station to remote server
Convert ECG Data
Encrypt data with elliptic curve cryptography
Verify original and encrypted data
Receive and verify the data
Perform Authentication
Forward information
Encrypt data with HIGHT
Verify authentication
Users view the data

Fig. 3. Overall flow of proposed method

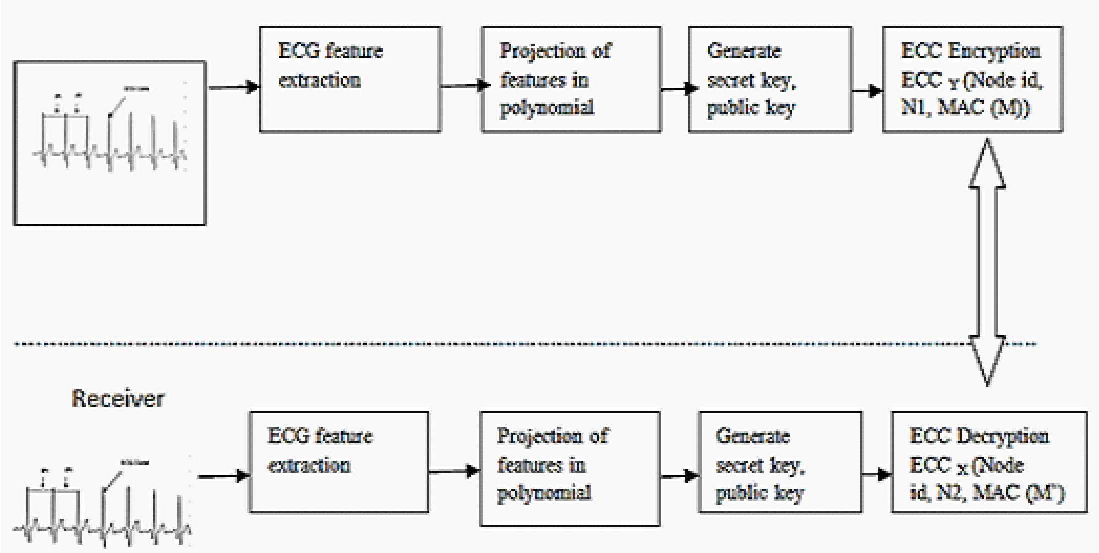
ECG feature extraction
Projection of features in polynomial
Generate secret key, public key
ECC Encryption ECC Y (Node id, N1, MAC (M))
Receiver
ECG feature extraction
Projection of features in polynomial
Generate secret key, public key
ECC Decryption ECC X (Node id, N2, MAC (M')

Fig. 4. Process of ECC in ECG signal

sensor head encrypt the message using base station's public key. The lists of all available base station public keys are available in all sensor head nodes. The encrypted message contains node id, session key value and hash value of message. The base station decrypt the data using it's private key .The base station compares sensor head node id contained in the message with sensor head id stored in its database. If the node ids are matched, the sensor node is allowed to transfer the data to the base station.

Each SH aggregates data from the local sensors and send the head node id to the BS. The node id is encrypted with BS's public key. The BS decrypts the node id value and verifies the ID with list of node ID are stored in the BH. If it is successful, the BH send the random number value to the BH This random number is encrypted with SH public key. The SH decrypt the information with its private key. The SH increment the random number value and send it to the BS .The BS verifies the sequence of random number and send the acknowledgement to the SH. Now, the SH send the session key which is encrypted with the BS public key (BS_y) and the information of data is sent to the BS. It is given by

$$SH \rightarrow BS : E(S_{id})BS_y \quad ...(4)$$

$$BS \rightarrow SH : E(R1)SH_y \quad ...(5)$$

$$SH \rightarrow BS : E(R1+1)BS_y \quad ...(6)$$

$$BS \rightarrow SH : E(Ack)SH_x \quad ...(7)$$

$$SH \rightarrow BS : E(\ M, S_{id}, D_{id}, BS_{id}, Key_{session}\ )BS_y \quad ...(8)$$

Transmission Between The Base Station To Remote Users

Design of HIGHT Encryption using ECG Key:

HIGHT was proposed by Hong *et al.* in 2006 .It is a generalized Fiestel network with a block size of 64 bits, a 128 bit key and Feistel structure with 32-rounds having uncomplicated XOR functions , modular expansion in the 28 elements group, and rotation in bitwise. The HIGHT was developed speciffically for lightweight cryptography. The lack of conventional substitution layer, its Feistel structure and byte oriented functions make it suitable for minimal effort, low-control, security investigation and lightweight usage. The designers of HIGHT show resistance against differential, linear, truncated differential, impossible differential, saturation, boomerang, rectangle, interpolation and higher order differential, algebraic attacks and their related-key variants. Therefore, HIGHT is most suitable for low energy, fastest and highly secure encryption technique to implement in WSN or BAN.

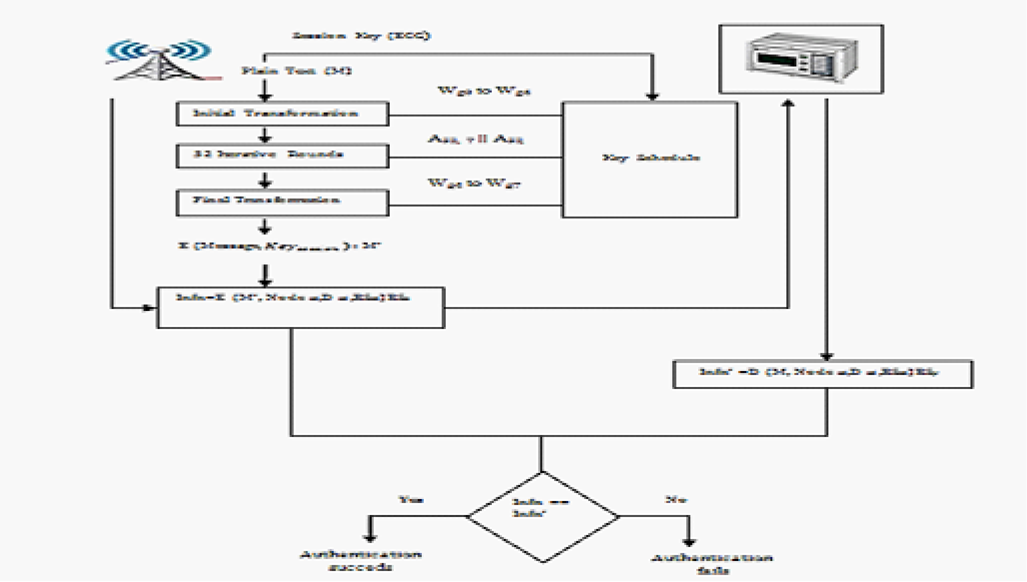

Fig. 5. ECG Signal Based Key Generation and Effective Key Exchange Protocol

Encryption

In this paper, HIGHT cryptographic algorithm is used to ensure the secure transmission and ECG signals are utilized for master keys. Here, we focused only on the encryption process HIGHT because the decryption process is explained in the similar to the encryption process. The encryption process of HIGHT consists of key schedule, initial transformation, round function, and final transformation. Its description is as follows.

The key schedule for HIGHT describes the procedure to make whitening key bytes W_{Gi} and 128 subkey bytes M_K from a 128-bit master key K = K15 || K14 || ... || K0, The master key is generated by using ECG Key generation method. The ECG key generation method can be done by whitening key Generation and Sub key Generation. The whitening key Generation uses 8 whitening key bytesWG0 to WG7 for the initial and final transformations. The Sub key Generation uses 128 sub keys are used for encryption and decryption, 4 sub keys per round. The encryption process has been takes place in Initial Transformation, Round function and Final Transformation. Initial Transformation transforms a plaintext P into the input of the first Round Function, ($A_0 = A_{0,7} \,||\, {}_{A0,6}$ …..|| $A_{0,0}$)by using the four whitening-key bytes, W_{g0}, W_{g1}, W_{g2}, and W_{g3}.Round Function uses two auxiliary functions F_0 and F_1. The Final Transformation untwists the swap of the last round function and transforms $A_{32} = A_{32,7}$|| A32, 6||…..||$A_{32,0}$ into the cipher text C by using the four whitening-key bytes W_{g4}, W_{g5}, W_{g6}, and W_{g7}.

The session key and information are encrypted with the base station private key(B_X) and the medical information is encrypted with session key which is derived from ECG signal using HIGHT algorithm sent to the remote server. It is given by

$$C_i = \mathrm{E}(\mathrm{Message}, Key_{session}) \quad ...(9)$$

$$BS \rightarrow RS : E(C_i, Node_{id}, D_{id}, BS_{id}, Key_{session})BS_x \quad .(10)$$

The base station generates the encrypted data with session key and again encrypt the encrypted data ,doctor id and node id with base station private key.

Decryption

The decryption process of HIGHT is carried out in the canonical way to invert encryption process. Key schedule creates the sub keys in the reverse order. The round function in the decryption process has Insub rather than Inadd and byte-swap with the inverse heading to that in the encryption process. The initial and the last transformations are performed by utilizing the information way of the round function with utilization of two additional multiplexers M2 and M3. The locations for both transformations are produced by C3. The initial transformation is performed while the information is, no doubt stacked into the shift register which spare clock cycles. The sub keys are created on the fly in both encryption and decryption forms. Here one and only 128-bit register is needed for both encryption and decryption which is generated based on ECG signal. The base station sends the encrypted data,sesson key value, docter id and base station id to the remote server. The remote server decrypt the information using base sation public key and get the encrypted data, session key.

$$RS \rightarrow BS : D((E(Message), Node_{id}, D_{id}, BS_{id}, Key_{session})BS_y \quad ...(11)$$

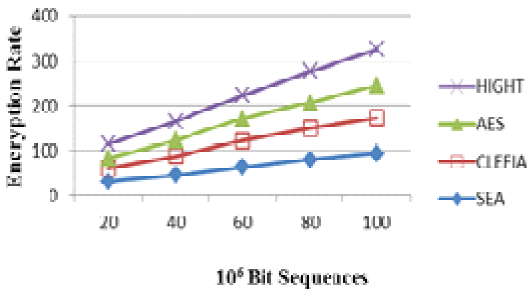

Fig. 6. Encryption rate Vs. Bit sequences for HIGHT and ECG technique

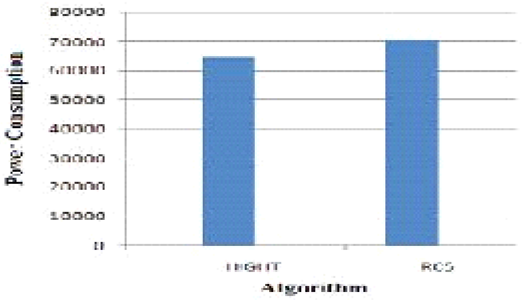

Fig. 7. Power Consumption

Thus the Secret key and the information obtained from the HIGH security and light weight Encryption and Decryption process undergo the Data authentication and secure key exchange process to send the information efficiently in secure way from the Base Station to the Medical Server and it is shown in Fig 5.

LogIn phase

When a user want to access the database, he has to login in to the database. The user first submits the ID and password (PW) to the login system. After receiving the information, the system checks the ID present in the database. If it is exist, it will calculate the hash value of ID and PW to base station. Otherwise, it will send the rejection message to the user.

$$M = H(ID||PW) \qquad ...(12)$$

After receiving the message=(ID, M) from the login system, the base station checks the ID present in its database. If it is present, then send accepted message to the login system.

Performance analysis

In this performance analysis, we evaluate the impact of reliable data transmission and security using clustering and HIGHT technique. The clustering technique provides energy efficient and authenticated data transmission. In clustering the Energy efficiency is more efficient when compared to other proposed schemes. And ensuring the security analysis using the HIGHT technique based on the Encryption method and compares the encryption rate with another Encryption technique. It represents the Encryption’s maximum delay according to the clock cycles per block and specifies the throughput based on the area. Here analyzing the comparison table, implementation results and graphs to achieve the better performance in Wireless Body Sensor Network.

Analysis of Clustering Technique

The communication range of each node is fixed at 10 meters. The energy consumption due to transmission of a packet by sensors or gateway nodes is considered to be 0.2 joules. It is to be noted that our schemes consider only upstream communication, *i.e.*, only sensors transmit data to their neighbour sensors or to its cluster head as the gateway. If numbers of deployed nodes are increased then the data transmission rate decreased, here using the clustering concepts to achieve the reliable data transmission. Energy consumption in authentication is less than the energy consumption due to confidentiality implementation. Presently, most clustering protocols expect a settled cluster transmission range, which brings about uniform cluster sizes. This methodology is compelled by the greatest conceivable sensor transmission range and the supporting MAC layer and determines the hub clustering is a helpful topology-administration methodology to decrease the correspondence overhead and endeavor information collection in sensor systems. The Fig 6 shows the Energy Efficiency with the accessing of number of nodes using clustering in BSN and Shows the authentication. This illustrates that the Body sensor network with cluster formation increases the energy efficiency and authentication between the sensors gets improved through the cluster formation in Body sensor network.

Analyzing of security parameter

For analyzing the security issues, the performance of the proposed Lightweight Security is evaluated using java. The encryption rate is shown in fig.6 is deployed in an area of 100 samples x 10^6 bit sequences is considered. Our circuit processes one round encryption per one clock cycle, thus its data throughput is about 150.6 Mbps at an 80 MHz clock rate. Note that our circuit is not area-optimized, and in order to reduce the timing, we can simply modify it to process 1/2 or 1/4 of one round operation per a clock cycle. The HIGHT Encryption Technique is compared with AES Encryption techniques. The result is shows in the following Table 2, which illustrate the maximum delay time, clock cycle and Throughput etc.

The fig.7 illustrates the proposed HIGHT technique which requires less power consumption per CPU cycle .The Table 2 describes about the comparison of RC5 and HIGHT techniques with respect to memory status, and power consumption. The comparison depicts that HIGHT techniques is efficient in minimizing power consumption, compared to RC5.

CONCLUSION

In this paper, we improved the security and reliable communication of data in WSBN by utilizing clustering technique combine with light weight (HIGHT) cryptographic algorithm. The clustering techniques minimize the energy consumption which increase the lifetime of sensor node in network, and balance the reliable communication among the nodes. The HIGHT cryptographic algorithm was designed to place in the energy constrained environment and it provide enough security for transmission of data in WSBN. Our performance analysis show clustering enhance the rate of efficient data transmission in WSBN and security analysis show HIGHT having greater security in WSBN, when compared with other cryptographic algorithms. In future, more efficient clustering technique can be proposed to reduce communication load in WSBN.

REFERENCES

1. Jin Soo CHOI and MengChu ZHOU, “Recent Advances in Wireless Sensor Networks for Health Monitoring”, *International Journal of Intelligent Control and Systems,* 2010*;* **15**(4), page(s):49-58.
2. Feng Xia, ZhenzhenXu, Lin Yao,Weifeng Sun and Mingchu Li, “Prediction-based data transmission for energy conservation in wireless body sensors”, Wireless Internet Conference (WICON), 2010 The 5th Annual ICST. Date: 1-3 Mar 2010, On 1-9
3. Tal Anker, Danny Bickson, Danny Dolev and BrachaHod, “Efficient Clustering for Improving Network Performance in Wireless Sensor Networks” Springer Berlin Heidelberg, DOI:10.1007/978-3-540-77690-1_14, Vol.4913, 2008, page(s) 221-236.
4. DeukjoHong,Jaechul Sung, Seokhie Hong,Jongin Lim,Sangjin Lee,Bon-Seok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, KitaeJeong1, Hyun Kim, Jongsung Kim and SeongtaekChee, “HIGHT: A New Block Cipher Suitable for Low-Resource Device”, Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, DOI:10.1007/11894063_4 , Vol. 4249, 2006, 46-59.
5. Krishna Kumar Venkatasubramanian, Ayan Banerjee, and Sandeep K. S. Gupta, “EKG-based Key Agreement in Body Sensor Networks”, INFOCOM Workshops 2008, IEEE, and Date:13-18 Apr 2008, On 1-6
6. G. Anastasi, M. Conti, M. Francesco, and A. Passarella, “Energy conservation in wireless sensor networks: A survey,” *Ad Hoc Networks,* 2009; **7**(3); 537-568.
7. Heinzelman, W.R., Chandrakasan, A.P., Balakrishnan, H., “An application-specific protocol architecture for wireless microsensor networks”, IEEE Transactions on Wireless Communication, DOI: 10.1109/TWC.2002.804190, Vol 1, No.4, 2002, 600-670.
8. E.Jovanov,A.Milenkovic,C.Otto,and P.C.Groen.”A wireless body area networks of intelligent motion sensors for computer assisted physical rehabilation.Jornal of NeuroEngineering and Rehabilation, 2005
9. Carmen C. Y. Poon and Yuan-Ting Zhang, The Chinese University of Hong Kong Shu-Di Bao, The Chinese University of Hong Kong and Southeast University” A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health “IEEE Communications Magazine , April 2006
10. Cherukuri,K.Venkatasubramanian, and S.Gupta,”Biosec: A biometric based approach for securing communication in wireless networks of bio sensors implemented in the human body” in *Proc.IEEE Int. Conf. parallel Process.Workshop,*Oct 2003,pp.432-439.
11. TassosDimitriou, KrontirisIoannis, “Security Issues in Biomedical Wireless Sensor Network”, Applied Sciences on Biomedical and Communication Technologies, 2008. ISABEL ’08. First International Symposium on Publication Date: 25-28 Oct. 2008 On 1-5
12. Y. W. Law, J. M. Doumen, and P. H. Hartel. “Benchmarking block ciphers for wireless sensor networks extended abstract)”. In first IEEE International Conference onMobile Adhoc and Sensor Systems (MASS), DOI:10.1109/MAHSS.2004.1392185 , Oct 2004 On 447-456.
13. D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. S Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee.,”HIGHT: a new block cipher suitable for Low-Resourcedevice”, Proceedings of CHES 2006, *Springer,* 2006; **4249**, 46-59.
14. L. Biel, O. Pettersson, L. Philipson, and P. Wide, “ECG Analysis: A New Approach in Human Identification,” *IEEETransaction on Instrumentation and Measurement,* 2001; **50**(3); 808–812
15. S. Cherukuri, K. Venkatasubramanian, and S. K. S. Gupta, “BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body,” *In Proc. of Wireless Security and Privacy Workshop,* 2003; Page(s). 432–439,
16. Md. MokammelHaque, Al-Sakib Khan Pathan, and ChoongSeon Hong, “Securing U-Healthcare Sensor Networks using Public Key Based

Scheme", ISBN 978-89-5519-136-3, ICACT 2008 Feb. 17-20, Page(s) :1108-1111.

17. AlokRanjanPrusty ," The Network and Security Analysis for Wireless Sensor Network: A Survey", *International Journal of Computer Science and Information Technologies*, 2012; **3**(3); 4028 – 4037

18. D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. "Medians and beyond: new aggregation techniques for sensor networks",. Proceedings of the 2nd inter- national conference on embedded networked sensor systems, ACM Press 2004, Pages 239-249.

19. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Communications Surveys Tutorials*, 2006; **8**: 2–23.

20. Wander, A.S., Gura, N., Eberle, H., Gupta, V., and Shantz, S.C., "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", *Proceedings of percom,* 2005; 324-328.

21. Keith M. Martin and Maura Paterson, "An Application-Oriented Framework forWireless Sensor Network Key Establishment", *Electronic Notes in Theoretical Computer Science*, (2008); **192**: DOI:10.1016/j.entcs.2008.05.004, 31–41

22. Seyit A. C¸ amtepe and B¨ulentYener. "Key distribution mechanisms for wireless sensor networks: a survey", Technical Report TR-05-07, Rensselaer Polytechnic Institute, March 2005.

23. Kalpana Sharma, M.K. Ghose and Kuldeep, "Complete Security Framework for Wireless Sensor Networks", *International Journal of Computer Science and Information Security"*, 2009; **3**(1).

24. Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and Pingxin Zhang, "Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks", *IEEE Journal of Biomedical and Health Informatics*, DOI: 10.1109/JBHI.2012.2235180, 2012

25. S. Mollera, T. Newe, and S. Lochmann, "Prototype of a secure wireless patient monitoring system for the medical community," *Sens. Actuators A: Phys.*, 2012; **173**(1) 55–65.