International Journal of Scientific and Research in Engineering (IJSRE)

Home Page: https://ijsre.org

A Novel of High Secure Protocol Architecture for Healthcare Wireless Body Area Network

K. Uma[1, *], Thirumurugan Shanmugam[2]

[1] School of Information Technology and Engineering, VIT University, TamilNadu, India. uma.kuppusamy@vit.ac.in

[2] Department of Information Technology, College of Applied Sciences Suhar, Oman. thirumurugan.soh@cas.edu.om

*** Corresponding author.**
E-mail: *uma.kuppusamy@vit.ac.in*

Article History:
Received Date: 08 March 2024
Revised Date: 04 March 2024
Accepted Date: 17 April 2024
Available online Date: 27 April 2024

Keywords:

Medical Wireless Body Area Network (MWBAN); Healthcare; Security; Hospital; Encryption; Data Transmission

ABSTRACT

The distributed wireless sensor network technologies have become one of the most important research areas in health care due to the rapid maturity of improving quality of life. The Wireless Medical Sensing Network (MWSN) enables long-term monitoring of vital health parameters, allowing doctors to make a more accurate diagnosis and better treatment. MWSNs provide flexibility and cost savings for patients and the healthcare industry. Medical patient sensors are generating more and more real-time data. The transmission of these data over wireless networks in the hospital has become a serious problem as one person's health information is highly sensitive, confidential and confidential. In this paper, we provide security models that protect the transmission of medical data to hospitals using MWSN. We offer encrypted encryption to transmit secure, low-lifetime information through sensor networks.

1. Introduction

Wireless Body Area Network (WBAN) is a network of autonomous sensing equipment commonly used in known locations, such as radio signals, sound, temperature and more. Watch and collect. WSNs can be used in a variety of industrial and civil applications, including industrial process tracking and monitoring, health applications, habitat monitoring, and countless other automation. Today, the health system is extremely complex. The number of older people and those who need continuous treatment is increasing day by day. Doctors face increasing challenges every year. This raises serious questions of interest that need to be answered best. Problem-solving should include a detailed analysis of the current situation to provide an adequate and functional framework for solving a sufficient number of issues [1]. Medical wireless sensor networks can provide this solution. Modern health systems use portable and implantable medical devices to hold patients, transmit medical information, record vital patients and organize organs. Medical wireless biosensor systems can help people with health services such as medication, memory expansion, home screening, access to emergency medical information [2]. Moreover, the application of new technologies in health applications, regardless of safety, often enables the patient to provide real data. For example, the physiological signs of a viable patient are very sensitive (i.e., the patient has an unpleasant disease), so the outbreak of some diseases can scare him. Collecting and using potential opponent data from patients may be life-threatening for the patient or may disclose the patient's private affairs. For example, in a basic situation, the patient's body sensors transmit the information to the health care provider/parent body. In the meantime, the attacker can listen to the patient's data while transmitting the data and invading the patient's privacy. This attacker can then post tolerant

information about social destinations (Facebook or Twitter, etc.) and therefore pose a threat to patient protection.

The conventional security mechanisms require unlimited resources and therefore cannot be applied directly to resource-related end-of-tunnel sensors. While the MWSN has the same security requirements as conventional networks, namely availability, confidentiality, integrity, authenticity, data freshness, and failure. In this way, security protocol resources have emerged as one of the most important problems in medical applications using medical wireless sensor networks [3]. Previous security research is ongoing along with data security issues for wireless health applications. To reduce security issues, considering the resource bottlenecks of wireless sensor networks, we recommend an efficient solution for data transmission in this article. Our application combines Compression Recognition (CS) with encryption and reliability. Compressed capture is a revolutionary idea recently to achieve a much lower sampling rate of weak signals such as physiological signals. Therefore, CS theory, like MWSN, seems to be an attractive solution for accessing low-performance independent networks. Also, our speculative expertise shows that the proposed structure meets the requirements [4].

The article is interrupted as follows. In Part 2, we look at some of the linked work. Part 3 describes the proposed plan, while Part 4 describes the proposed protocol. Security aspects are discussed in Chapter 5. The results of the safety performance analysis are discussed in Chapter 6. Finally, Section 7 concludes with final considerations and future work.

2. Related Work

In the sensor, application security issues have always been part of the action study. Of late, remote sensing security issues were the most critical areas of research. Some, such as [5] and the like [6], specifically focus on health problems related to health applications.

The Elliptic Curve Cryptography (ECC) becomes a viable public key encryption option for wireless sensor networks. The main reason for this is relatively fast computing, small size, and compact signature. There have been many noteworthy contributions in recent years. One of the earliest works on ECC sensor networks is Malan *et al*. [6]. There is a group of people involved in this work, the keyframe with ECC being implemented and evaluated in the bit phase of the Mica2 sensor. Uhsadel *et al*. [7]. Recommends the effective implementation of the European Neighborhood Policy. Recently, Szczechowiak *et al*. [8] Recommended by Nanotech, which is moderately faster than current ECC usage but regularly requires huge ROM and RAM measures.

Malasri *et al*. [9]. It provides a wireless medical detector solution that: (i) ECC-based security exchange protocol for key exchange to create shared keys between sensor nodes and base stations; (ii) Symmetric encryption and encryption to protect the confidentiality and integrity of data; III. Certification system for checking data source. Oliveira *et al*. [10]. Offers Tiny Tate, a lightweight security system for conventional remote sensing systems (IBE). Tan *et al*. [11] Recommended WBAN encryption security solution. In their work, sensor nodes calculate public keys when using the hash function as a function of generation keys. These keys are stored in flash memory and used to encrypt/decrypt elliptic curves using the Elliptic Curve Digital Signature (ECDSA) algorithm. This approach has several disadvantages: increased runtime increased power consumption due to increased computational costs, and greater storage of public key flash keys Also, IBE-Lite offers personality-based cryptography [12]. The balance between security and availability. However, we can see that IBE-Lite has security flaws and performance issues. First, ECC encrypts all medical data that is ineffective for MSN. Second, their job does not count sensor credentials in the sink (or user). In this way, false medical data can be entered or legally processed due to a lack of detection of difficulties.

L. Zhou *et al*. [12] actualized by the new Romantic Road Safety Architecture, underlining the key components of a media-agreeable street wellbeing design, which is key administration, bunch rearrangement, acknowledgment, and watermarks. They rank the most significant administration relying upon how the sight and sound traffic is overseen, contingent upon whether the framework is versatile or not, and change the key dependent on synchronization and execution [13], M. Khalid and A. Al: Specialized and regulatory measures ought to be taken to meet the information insurance and security goals to guarantee consistence with the security prerequisites of the electronic wellbeing record framework. Their research shows that many countries have started to switch to electronic health records and national health records. It is argued that full protection of the eHealth network is at the heart of today's scientific circles.

3. Proposed System Architecture

The contingent upon the application circumstance, therapeutic sensors are utilized autonomously. Oneself controlled remote detecting association comprises of little remote concentrators that are situated on or close to the patient's body and together give the application limit required by the application. In the most straightforward case, the focal PC gathers and stores sensors, for example, ECG, EMG, EEG, SpO2, and circulatory strain (systolic and diastolic).

3.1. Network model

The situation plot in Figure 1 is the emergency clinic organizes. The proposed design comprises of four sections:

The therapeutic sensors related with every patient, the sensor hubs, can be situated on or close to the patient's body and discuss remotely with outside control gadgets; The Bedside Patient Access Point (PAP) has expanded registering power, battery control, and systems administration capacities. This hub gathers totaled and accumulated information from therapeutic sensors, approves the information, and transmits the prepared information to the best base station; The BS fills in as an extension between the PAP and the PC server, permitting association among patients and remote social insurance suppliers, and transmission of therapeutic information and control messages. On the PC server, the client can see the graphical UI used to send directions and solicitations to arrange motors, empowering social insurance experts to remotely screen their patients progressively in a versatile situation. All wellbeing parameters can be put away for additional data. Joined with ongoing wellbeing parameters, doctors and parental figures can give helpful medicinal consideration to their patients.

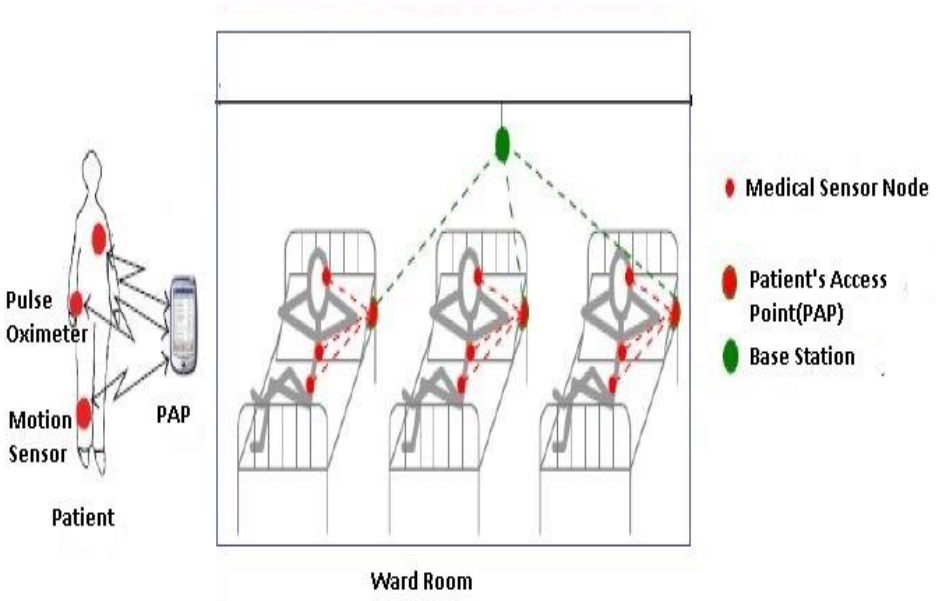

Fig. 1. Wireless Body Area Network Proposed Architecture for Hospital.

Figure 1 shows the components described in the following subsections:

- *Medical Sensor node (MSN):* Made from small distant centers in or near the human body, these sensors detect pulses (systolic and diastolic) of ECG, EMG, EEG, SpO2.
- *Patient's Access point (PAP):* The patient's aggregator is attached to the bed. Enables encryption of encrypted data and authenticates encrypted messages.
- *Base Station (BS):* It is responsibly designed to send information from paths to sensor nodes; otherwise, it receives data from the server.
- *Server:* The server receives all packets from all network controllers in the network. The server processes the data, stores it in a database, and presents it in an appropriate interface format. The platform is an

open and expanding platform that enables easy integration of tools from different manufacturers.

3.2. The requirement of a Secure System

In this section, we present several criteria that represent the desirable features of a secure MWSN system.

- *Confidentiality:* To ensure that patient information is leaked, the information must be kept secret on the hub or on a neighboring server (that is, a system server). Data confidentiality must conflict with device-related attacks (such as those attacked by the controller and packaged by the controller). This means that the threat of a node will help your opponent's gain some or all of the data stored in that node.
- *Authentication:* This is required by the MWSN to validate network nodes and thus prevent network compromises and/or fraud.
- *Data integrity assurance:* In the case of MWSN, patient data is vital and altered data can have catastrophic consequences. Therefore, the integrity of the data must always be protected.
- *Availability:* Because this network provides extremely sensitive, important, and potentially life-saving information, you should always have network resources.
- *Privacy:* the patient's data must not be disclosed to unauthorized persons (individuals). Medical information is one of the most common and non-public statistical sets. The system must employ mechanisms that will be able to comply with applicable and potential laws while regulating the confidentiality of personal data.
- *Fine-grained data access control:* Access control should apply to patient information through the MWSN to prevent unauthorized users from obtaining personal information. More importantly, a security system must have different permissions for different network users.

4. Proposed Protocol

The essence of the work is the secure transfer of data between the SNs and the server. The proposed system is discussed in five stages.

4.1. Phase 1: System Setup

After installation, the network is trusted for a short time, so each sensor initializes (i) the PAP and BS definitions to send reports to the PC server. At this point, each node (sensor or PAP) sends multiple health messages. The sensor collects these messages and knows the PAP and BS. Each sensor sends a message (ID) with the touch node ID and the node coordinate point.

These IDs were encrypted and sent to the PC server via PAP and BS. At the end of the phase, the PC server can create a mapping table to record the PAP of each sensor. Because of the dynamic behavior of WSN, the computer server must regularly call the system setup process to update the mapping table. Since implementing such a process requires additional energy costs, the computer server should consider whether it can be done. In this paper, it is assumed that the sensors are quasi-static after they are scattered so that the adjacent sensor connection is relatively stable. This means that the computer server can only call the system setup process when new sensors are found.

4.2. Phase 2: Compressed Sensing

We will probably try to reduce the cost of living, including living costs, mailing costs, and registering nature versatility in every possible way. First, the compression sensor (CoS) is compressed. The encoding is done before it is transmitted to the channel. Integration is also protected by a hash algorithm to prevent malicious changes [14]. The combination of CoS theory and WSN results in promising improvements in some limitations. CoS optimizes energy consumption, an important factor for WSN.

In our model, we investigate the network of N detector nodes. The number n of each node is between 1 and N. We assume that the signals generated by personal health records (PHR) are positive real numbers. It is also assumed that the occurrence is occasionally scattered [15]. With the Centered Exakt algorithm and every time interval, each node touches the environment and passes the scan to the computer server. As a result, N intervals can be collected on the computer server for each interval. N × T data can be collected at T intervals. These values can be arranged in the N × T matrix, where the line and segment numbers compare to the hub ID and time field number. Thus, just a bit of the read from every hub is transmitted to the PC server, which has different

advantages, for example, diminished transfer speed and longer life. The encoding calculations for every sensor are portrayed underneath.

Step 1: Each sensor node generates a random binary vector at the PV sampling position, only p (p <N) with non-zero entries. Here we call the β = [N / p] sample ratio MCo (Matrix Completion).

Step 2: Then each sensor node examines the binary vector of the sampling position and appears only if the corresponding entry is not zero. Finally, these sample models form a vector 〖X〗 _p∈R_p. This step uses MS-based compression. Each node estimates only the p-value of N, which results in a compression ratio β = [N / p]. This reduces the cost of sampling energy.

Step 3: First, each sensor node creates and stores the same rare binary matrix as the previously distributed E core between 〖S〗 _pXq (p <q), the E sensor, and the sink. Only a small number of d (p>d≥1) non-zero elements are randomly located in each column 〖S〗 _pXq. In addition, the CoS compression ratio is called γ = pq.

Step 4: Each sensor center receives CS_ estimates from Y_p and X_q that are equivalent to the operation: Y_p = S_pXq × X_q After passing through Y_p and transferring the vector of the PN test situation, it returns to step 1. In this process, since our evaluation framework is a rare dual network, the cost of living for this CS pressure is related to direct expansion.

Although X_q is a random sample of N continuous reads and due to time correlation, it has been found that X_q is still rare in some transformations. Therefore, you can use CS to compress post-compression data based on the Matrix Completion. Finally, each sensor must send q values instead of N values, resulting in a full pq = β × γ compression. Messages must be encrypted for secure data transmission.

4.3. Phase 3: Encryption

This section provides a very simple algorithm for updating each key. The unique key for each sensor is the transmission of a dynamic personal health record (PHR) extract to update the dynamic key. The idea that PHR is used as a key agreement is the observation that the human body is dynamic and complex, and that the PHR is at the same time unique. In this way, the PHR updates each key to ensure good randomness so that the opponent does not recognize or compromise system security.

Toward the part of the arrangement, the individual key of hub S_i is registered as,

$G_i^t = G_i^{t-1} \oplus h(PHR_i^t) \quad t=1, 2\ldots$ (1)

Where PHR_i^t implies the PHR from center point MSN_ito PAP at round t while h (⊙) is a confined hash work which is openly known.

At that point, G_i^(t-1) is securely erased. Review that G_i^0 (=G) is the underlying individual key utilizing the polynomial offer, we reinterpret (1) as$G_i^t = G_i^{t-1} \oplus h(PHR_i^t) = G_1^0 \oplus \oplus_{n=1}^{t} h(PHR_i^n)$ (2)

Condition (3) is equivalent to Shannon's one time pad encryption. Exactly when key spillage occurs (e.g., center point Si is jeopardized), the foe knows 〖 G〗 _i^0. For this circumstance, ⊕_(n=1)^t h(PHR_i^n) goes about as the one time pad to keep the foe from concluding 〖 Gi〗 _(i)^t.

Accept that at round t, a biosensor hub, say MSN_i, plans to convey the information thing $\{DATA_i^t\}$ to PAP. Node MSN_i generates the ciphertext CT_i^t as follows:

$CT_i^t = E\left(\left(\{DATA_i^t, t\}, G_i^{t-1}\right), h(DATA_i^t, G_i^{t-1})\right)$ (3)

It tends to be seen from focuses (1) and (3) that the PHR coding codes are refreshed each time another PHR is gotten. Encryption keys are never reused, in this manner restricting the danger of key exposure assaults. At that point, node

〖 MSN〗 _i, conveys {CT_i^t, 〖 ID〗 _(MSN_i), 〖 ID〗 _(PAP_i) } to PAP. Note that PAP can likewise refresh the one of a kind key with the MSN_i hub. The above figuring mirrors the utilization of the area since family unit XORs and hash errands are quickly picking up quality with most pictorial gadgets. Additionally, the computational expense is low because of the straightforwardness of the calculations.

4.4. Phase 4: Aggregation $\boldsymbol{PAP_i}$ to $\boldsymbol{BS_i}$

Each PAP collects messages from all patient sensors. Because of the use of PHR, PAP and BS must be able to directly encrypt the encrypted data. Recovery remote sensing systems are made from small devices, with limited computing and limited viability. For such devices, data transfer is a very energy-intensive operation. In this way, the lifetime of the MWSN essentially limits the number of bits sent from each module. An added

homomorphism is used to protect the materials to allow for the conglomeration of confusing information. The goal of homomorphism in the protection of added materials is to accumulate vital information by reducing unnecessary transmitted messages. The information package has been further developed to work with homomorphism encryption [16]. Several cryptosystems with homomorphism and their variants are found in the text. Basic and proven, it provides a tide of homomorphism that provides efficient, encoded information. The primary thought of the arrangement is to supplant the Xor (Extremely OR) task, regularly found in stream expansions with the deliberate augmentation (+). We currently give a short portrayal of this cryptosystem [17].

Let T be a large integer and S be a secret key. To encrypt message m < T with S, we calculate,

$$E_S(m, S) = (m + S) \bmod T \quad (4)$$

To decrypt a cipher-text c with k, we calculate:

$$D_M(c, S) = (c - S) \bmod T \quad (5)$$

It is obvious that the modular encryption is additively homomorphism, i.e.

$$E_M(m_1, S_1) + E_M(m_2, s_2) = E_m(m_1 + m_2, k_1 + k_2) \quad (6)$$

The information accumulation is performed utilizing the whole administrator and the outcome is transmitted when the aggregator gets the data from generally sensors. It utilizes a break to avoid the aggregator to remain persuaded. Maintenance time relies upon the aggregator's situation in the framework and a few sensors will be unable to report.

4.5. Phase 5: Aggregation BSi to PC Server

Every BS gathers total information from all PAPs in patients. Each BC Tg transmits the combined information to the PC server after a period. So, BS needs to stand by longer than PAP. The time move is meant as Δtg, which is in the tuning stage.

The server gets just a single data parcel, which comprises of graphical substance with respect to the PHD of a noteworthy number of sensors in the framework. To start with, the server translates the information and gets the PHD1, PHD2 ... PHDr successions. In the wake of decoding and confirming the information.

Subsequent to tolerating the PHD, the PC Server checks the truth of every sensor. We additionally suggest a low-intricacy control framework that can be applied to hubs at all three degrees of the system. Every PAP doles out an extraordinary ID number to every sensor that is situated in your patient. Also, every PAP has a novel identifier and every BS has an interesting identifier. It ought to be noticed that the quantity of PAPs and BSs inside the system is little contrasted with advanced sensors (MSNi). Likewise, they have higher capacity, power and registering abilities than MSNi. On the off chance that the above check comes up short and a mistake happens, a notice message will be produced.

5. Security Analysis

Security is a significant part of any system. Particularly when executing MWSNs, classified treatment of delicate wellbeing information is fundamental. Deception of individual data influences its exactness and can be destructive to the patient. Additionally, obstruction from different machines or systems can be a risk. Guarantee that the system incorporates significant confirmation issues (specialized gadget ID check), privacy (individual information bargain), trustworthiness (information/messages right and mistake free), and nearness (shortcomings and different assets). Be that as it may, this system puts more accentuation on the test of guaranteeing that information and information stay private and exceptional. Our design ensures the accompanying security highlights:

Confidentiality and Authenticity: The MWSN needs to guarantee the personality of the information obtaining hub in light of the fact that the data from the powerless hub can impact quiet administration. It is additionally significant that the information gathered from the genuine hub isn't disregarded. Unapproved or altered information may bring about improper treatment and damage to the patient. The uprightness of our methodology is guaranteed by the hash capacity determined for bundles sent between the PC server and each system sensor.

Confidentiality: MIPSN nodes provide highly sensitive medical information. Patient data is also needed for safe and secure data transmission. This aspect is provided by symmetric encryption to encrypt traffic exchanged between the computer server and the sensor nodes. Encryption must be done by automatically updating the keys.

Availability: The decision grants access rights to the services available to right holders, if necessary for real estate, to arrange a rectangular fair and good buyer event. He is also opposed to administrative wear and tear.

Corruption Resistance: The interceptor endeavors to get to restorative records of private and touchy patients. This assault can happen when a patient contacts a server or cloud supplier. Our answer sets up an entrance control framework and guarantees that clients (patients/wellbeing experts) don't consult with one another to increase unapproved access to restorative information. Our design opposes shrouded assaults to counteract unapproved access to therapeutic information.

Light and scalability: The framework just needs a light sensor. Thus, concerning the memory most remote from the sensors, just one refreshed symmetric key is embedded into each control board. In this way, the figuring and capacity necessities of the sensor are low. Likewise, the computational multifaceted nature of the sensor hubs (or system clients) doesn't rely upon the quantity of sensor hubs or system clients. Thusly, the framework can be adaptable.

6. Performance Evaluation

At this stage, the adequacy of the proposed framework is assessed by recreation. The topology of our system is appeared in Figure 2, where every hub has an identifier. The reenactments were performed in 100 patients in 10 rooms and every patient performed with the fitting PPA. This convention was created by TinyOS 2.0 (TOSSIM) and Power TOSSIM. We expect to give the required degree of security, at any rate by utilizing extra vitality [18]. To assess the power utilization of a PC overhead line, we look at two execution markers: framework control utilization and overhead line [19]. As appeared in Figure 2, the complete power utilization of the system can be evaluated by various pressure proportions. The recreation results demonstrate that our convention devours less control, up to 75% on the off chance that it is somewhere in the range of 0.6 and 0.9. This shows the proposed framework devours minimal measure of vitality contrasted with the correlation frameworks. These outcomes demonstrate that all remote power is fundamentally decreased by information pressure. This mirrors the instance of most sensor systems. A large portion of the vitality is utilized for radio recurrence correspondence, not for neighborhood preparing of the processor, because of the costly reception apparatus and numerous information records.

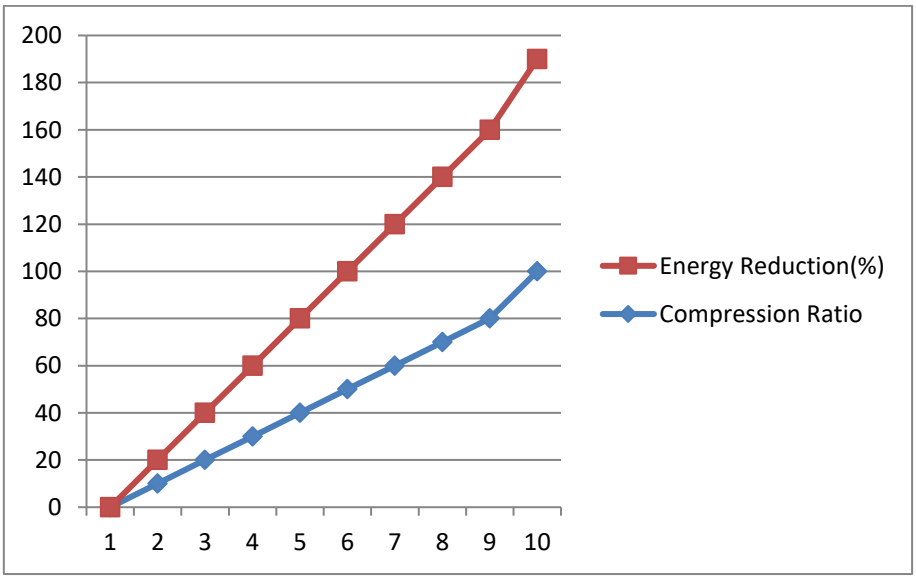

Fig. 2. Power reduction vs. Compression ratio

The compacted identification stage ensures a fair hub vitality cost by altering the measure of information transmission, which expands the life of the system.

7. Conclusion

In this paper, we examine manages information sent from therapeutic sensors to emergency clinic remote systems. To meet the asset prerequisites of the remote sensor hub, we present a protected transmission framework dependent on compacted location and encryption. The security investigation has demonstrated that our framework can meet the necessities of these kinds of conventions. With our model, we assemble a monetarily solid and powerful patient screening system. This framework empowers specialists to analyze patients remotely in a truly solid, dependable and safe way.

Acknowledgement

This research was not funded by any grant.

References

[1] B. Chandrasekaran, R. Balakrishnan, and Y. Nogami, "Secure Data Communication using File Hierarchy Attribute-Based Encryption in Wireless Body Area Networks," 2018. http://dx.doi.org/10.24138/jcomss.v14i1.446

[2] M. Compare and M. Hölbl, "Survey on security in intra-body area network communication," Ad Hoc Networks, vol. 70, pp. 23–43, 2018. ttp://dx.doi.org/10.1016/j.adhoc.2017.11.006

[3] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," Futur. Gener. Comput. Syst., vol. 78, pp. 956–963, 2018.

[4] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificate-less authentication protocol with anonymity for wireless body area networks," J. Netw. Comput. Appl., vol. 106, pp. 117–123, 2018.

[5] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," J. Med. Syst., vol. 36, no. 1, pp. 93–101, 2012. http://dx.doi.org/10.1007/s10916-010-9449-4

[6] Q. Pu, J. Wang, and R. Zhao, "Strong authentication scheme for telecare medicine information systems," J. Med. Syst., vol. 36, no. 4, pp. 2609–2619, 2012.

[7] L. Uhsadel, A. Poschmann, and C. Paar, "Enabling full-size public-key algorithms on 8-bit sensor nodes," in European Workshop on Security in Ad-hoc and Sensor Networks, 2007, pp. 73–86. http://dx.doi.org/10.1007/978-3-540-73275-4_6

[8] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the limits of elliptic curve cryptography in sensor networks," in Wireless sensor networks, Springer, 2008, pp. 305–320. http://dx.doi.org/10.1007/978-3-540-77690-1_19

[9] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments, 2007, pp. 7–12. ttp://dx.doi.org/10.1145/1248054.1248058

[10] L. B. Oliveira, D. F. Aranha, E. Morais, F. Daguano, J. López, and R. Dahab, "TinyTate: Identity-Based Encryption for Sensor Networks.," IACR Cryptol. EPrint Arch., vol. 2007, p. 20, 2007.

[11] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: an identity-based cryptography approach," in Proceedings of the First ACM conference on Wireless network security, 2008, pp. 148–153.

[12] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: lightweight identity-based cryptography for body sensor networks," IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 6, pp. 926–932, 2009.

[13] X. H. Le, M. Khalid, R. Sankar, and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," J. Networks, vol. 6, no. 3, p. 355, 2011.

[14] M. Balouchestani, K. Raahemifar, and S. Krishnan, "Low power wireless body area networks with compressed sensing theory," in Circuits and Systems (MWSCAS), 2012 IEEE 55th International Midwest Symposium on, 2012, pp. 916–919. http://dx.doi.org/10.1109/MWSCAS.2012.6292170

[15] P. Zhang, C. Chen, and M. Liu, "The application of compressed sensing in wireless sensor network," in Wireless Communications & Signal Processing, 2009. WCSP 2009. International Conference on, 2009, pp. 1–5. http://dx.doi.org/10.1109/WCSP.2009.5371386

[16] C. Castelluccia, A. C. F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks," ACM Trans. Sens. Networks, vol. 5, no. 3, p. 20, 2009. http://dx.doi.org/10.1145/1525856.1525858

[17] J. Domingo-Ferrer, "A provably secure additive and multiplicative privacy homomorphism," in International Conference on Information Security, 2002, pp. 471–483. http://dx.doi.org/10.1007/3-540-45811-5_37

[18] P. Levis, N. Lee, M. Welsh, and D. Culler, "TOSSIM: Accurate and scalable simulation of entire TinyOS applications," in Proceedings of the 1st international conference on Embedded networked sensor systems, 2003, pp. 126–137. http://dx.doi.org/10.1145/958491.958506

[19] 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, pp. 162–175. http://dx.doi.org/10.1145/1031495.1031515