International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/217707 Volume 9, Issue 6, November – December (2022)

RESEARCH ARTICLE

Privacy-Preserving Mechanism to Secure IoT-Enabled Smart Healthcare System in the Wireless Body Area Network

Renuka S. Pawar
Computer Department, Sardar Patel Institute of Technology, Mumbai, Maharashtra, India
renuka_pawar@spit.ac.in

Dhananjay R. Kalbande
Computer Department, Sardar Patel Institute of Technology, Mumbai, Maharashtra, India
drkalbande@spit.ac.in

Received: 12 October 2022 / Revised: 30 November 2022 / Accepted: 10 December 2022 / Published: 30 December 2022

Abstract – The IoT has been a subclass of Industry 4.0 standards that is under research from the perspective of quality of service (QoS) & security. Due to the pandemic situations like novel coronavirus smart healthcare monitoring gained growing interest in detection. In IoT data is communicated from Intra WBAN (Wireless Body Area Network) to inter-WBAN and then beyond WBAN. While transferring data from one layer to the other end-to-end data privacy is the challenge to focus on. The privacy-preserving of patients' sensitive data is difficult due to their open nature and resource-constrained sensor nodes. The proposed research design based on routing protocols achieves the patient's sensitive data privacy preservation along with minimum computation efforts and energy consumption. The proposed model is Secure Communication-Elliptic Curve Cryptography (SCECC) WBAN-assisted networks in presence of attackers is evaluated using NS2. The proposed privacy preservation algorithm uses efficient cryptographic solutions using hash, digital signature, and the optimization of the network.

Index Terms – Authentication, Cryptography, ECC, Encryption, Wireless Body Area Network, Routing Protocol.

1. INTRODUCTION

The smart healthcare system using the IoT enables hospitals to monitor their patient's health from any place in the world periodically [1]. Smart healthcare is mainly based upon Wireless Sensor Networks (WSNs) under which the patients have been equipped with body sensors & hence acts as a node in the network. Such networks are also defined as Wireless Body Area Network (WBAN). Because of the progressions in Micro-electromechanical systems (MEMS) and wireless correspondence advances, WBAN has experienced a specialized impact in the most recent decade. There are wide assortments of security assaults that are conceivable because of the wireless idea of the correspondence medium. Consequently, security must be given in the application layer just as in the network layer [2-4]. Through information security, the assurance of information from unapproved clients while information is being put away and moved benefits the people to control the assortment and utilization of individual information about them [5-7]. The security instruments for shrewd medicinal services or WBANs incorporate (1) Data stockpiling: Confidentiality, Integrity confirmation, Dependability, (2) Data get to Access control, Accountability, Revocability, Non-denial, and (3) Other: Authentication and Availability. Furthermore, the WBANs data will be available almost everywhere, anytime. Inescapably, & such data has been beggarly sensitive & problematic hence an attacker may insert malicious nodes under the network for leaking the body sensor's medical data (&/or involves false reports) except permission regards the network owner [8-11]. There are several access control policies introduced, however, selecting the appropriate approach to achieve privacy preservation is a challenging task considering the limited capabilities of sensor devices (constrained battery, low memory, less bandwidth, & lower bandwidth). How to address the privacy-preserving requirement of smart healthcare systems using WBAN-assisted IoT is a big forthcoming issue for many researchers. Designing the access control policies to address these issues needs to satisfy the requirements of energy efficiency along with strong security without disclosing the sensor's identity. The reason regards this research has been for describing designing & evaluation of access control policies-based routing schemes to achieve privacy preservation in the smart healthcare system. Along this connection, we first design the system model of a smart healthcare system using WBAN-assisted IoT in the presence of malicious nodes in the network. Secondly, the two existing access control protocols such as ACP and CDHSC] are described along the

RESEARCH ARTICLE

assumptions & constraints of their design. Third, the simulation results use various performance metrics that demonstrate the energy efficiency, QoS efficiency, & computational efficiency of investigated protocols.

1.1. Problem Statement

The access control policies for WBANs achieve the authentication and authorization for data security and privacy preservation using cryptography techniques. But using cryptography techniques introduces another challenge of energy consumption, communication delay, and overhead. The problem statement of this research is to present the consolidated routing solution that achieves security and privacy preservation with energy efficiency and network cost reduction. The problem statement of this research further extended performance trade-offs among the parameters related to energy efficiency, network QoS, and computational efficiency.

1.2. Objective

The objective of this research is as follows-

- Creating identities for the objects and people participating in the healthcare system.
- To put in place access control policies in the IoT for the health care system.
- Create a lightweight access control framework that protects privacy.

1.3. Organization of the Paper

An overview of the paper is presented in this section along with the problem statement and objective. In section 2, we have done the literature survey. In section 3, we have discussed the various lightweight protocols used during the proposed model section 4 proposed algorithm, section 5 results and discussion, and section 6 conclusion and future work.

2. RELATED WORK

The IoT-based design of e-healthcare applications received more attention from researchers. This design mainly depends on the design of sensor network protocols such as Medium Access Control (MAC) and routing protocols. The routing protocols received more attention for their energy and QoS performances than MAC protocols. As the routing protocols are responsible for route formation and data transmissions, most threats are introduced at the routing layer only. Therefore, it is required to design the access control policies for the routing protocol of resource-constrained networks like WBANs. This chapter presents a detailed survey on WBAN considering the e-healthcare applications. Various protocols for WBAN received designed for different objectives. The related works were then reviewed followed by the research gaps.

2.1. IoT-Enabled WBAN

The IoT-driven innovation called Body Area Network (BAN) or Wireless BAN (WBAN) is a network created for checking the ailments of a patient. It is as yet in an early advancement stage. Various clever physiological sensors can be consolidated into a wearable WBAN. The wearable sensors can be mounted or implanted in the human body. WBAN sensors are fit for checking, preparing, and imparting different imperative signs like ECG, pulse, and body temperature, without making any uneasiness in the patient. The data gathered by the wearable sensors will be sent remotely to an outer preparation unit, or, to the web. An average sensor node comprises a sensor, a processor, a handset, and a force unit. The sensor nodes constantly sense flags and forward them to the clinical worker. Sensor nodes in WBAN are battery-driven units that have restricted battery assets. WBAN offers two benefits: the portability of patients and the area-free observing office. The necessities of WBAN are precision, dependable correspondence, low force utilization, security, and the nature of administration. WBAN helps in distant patient checking in a solid and cost-powerful way. WBAN network will want to screen patients in their homes and work environments, along these lines, diminishing the cost and improving the personal satisfaction of the patients. This is a framework that can persistently screen the ailment of older individuals, and, offer the data too far off care suppliers or clinics. The embedded sensors will capture the data to be sent remotely to an outside handling unit.

2.1.1. Challenges

Wireless body area sensor networks (WBANs) are getting better known as continuously checking. Energy effectiveness and nature of administration (QoS), security, and privacy issues are significant concerns.

- Security: WBAN transmission should be secure and precise. It would need to be ensured that the patient "secure" information is just gotten from every persistent committed WBAN framework and isn't stirred up with other patients' information.
- System gadgets: The sensors utilized in WBAN would need to be less intricate, little measured, light weighted, power productive, simple to utilize, and reconfigurable.
- Data consistency: Data living on numerous cell phones and remote patient notes should be gathered and investigated in a consistent style.
- Interference: The remote connection utilized for body sensors, ought to diminish the obstruction and increment

RESEARCH ARTICLE

- the concurrence of sensor node gadgets with other network gadgets, accessible in the climate.
- Data Management: As BANs produce huge volumes of information, the need to oversee and keep up with these datasets is of the most extreme significance.
- Mobility: Due to the versatility of the human body, network geography is changed, thus, the course between the nodes will be mutilated or destroyed. If the course is broken, there is a chance of information misfortune.
- Limited energy source: The decrease in the size of wearable or implantable nodes warrants a decrease in battery size. In WBANs, energy is spent doing three significant undertakings: detecting activities, figuring out tasks, and correspondence over remote channels. A more modest battery restricts the capacity of a sensor node to achieve this, and, consequently prompts the disappointment of a node. The batteries should be re-energized or supplanted occasionally.

2.2. Security and Privacy Preservation Methods

Recently several access control policies were designed for sensor-based networks as security and privacy preservation measures with minimum computational efforts. This section presents the state-of-art methods for healthcare security using IoT-enabled WBANs or WSNs.

The reviews on various methods recently conducted in over security & privacy preservation for WBANs/WSNs. In [12], protection preserving decentralized cipher text-strategy attribute-based encryption (PPDCP-ABE) is proposed to enhance the protection & security in sensor networks. In [13], the author introduced the first methodology that considers shared authentication in two-tier WBAN. In [14], certificate-based encryption (CB-SN) scheme was proposed for the IoT-enabled WBAN. They utilized the concept of hyper-elliptic curve cryptography (HECC) that offers the same level of security as the elliptic curve & bilinear blending along lower-key size. In [15], an efficient certificate-less encryption method was proposed to design an access control scheme for the WBANs to achieve protection preservation. In [16], the author proposed a secured ACP for WSN. ACP was designed using Elliptic Curve Discrete Log Problem (ECDLP) & double trapdoor chameleon hash work which secures the WSN from malicious attacks such as node masquerading assault, replay assault, man-in-the-middle assault, & forgery attacks. In [17], another ACP protocol to achieve privacy preservation along with node privacy for the WSN, to protect the WBAN communications from attackers we are comparing this work with the proposed SCECC algorithm. In [18], Pairing Free Identity-based Two-Party Authenticated Key Agreement convention proposed & collects the experimental outcomes on WSNs using Relic-toolbox cryptographic library. In [19], a heterogeneous encryption method is to control the users' access patterns. They enabled users in a certificate-less cryptography environment to send a message to a sensor node in an identity-based cryptography environment. They designed an access control approach for WSN-assisted IoT using the heterogeneous encryption method. In [20], a secure & efficient access control method for WSNs is proposed in the cross-domain context of the IoT called cross-domain heterogeneous encryption (CDHSC), to protect the WBAN communications from attackers we are comparing this work with the proposed SCECC algorithm. They achieved KSSTIS (known session-specific temporary data security) as compared to previous access control methods reviewed. First and foremost, both techniques ACP and CDHSC are designed for IoT-enabled WSNs kind of networks. The other methods disclosed in the literature cannot be suitable for WBAN networks like ACP and CDHSC protocols; this is the main motivation behind selecting both protocols. For WBAN or WSNs, due to resource constraints, it is necessary to design lightweight security solutions with maximum security guaranteed, the outcome of ACP and CDHSC protocols justified the minimum energy consumption along with guaranteed QoS performances. The system models used in both methods consist of such as sensor nodes, coordinator nodes, and base station nodes. These entities are replaced by IoT nodes (replace sensor nodes), access points (replace coordinator nodes), and gateway nodes (replace base station nodes).

Table 1 Summary of Related Work

Ref no	Methodology	Pros	Cons
12	Each authority can operate autonomously and offer keys to each user for the secure transmission of data to sensor nodes.	Use set membership proof and anonymous key extraction protocol	The solution will consume too many computing resources in the process of generating keys
13	A novel convention to realize anonymous shared authentication & confidential transmission for star two-tier WBAN geography	Very low computation cost and energy consumption.	Focuses on two-tire WBAN and does not include user authentication

RESEARCH ARTICLE

15	Worked on authentication, confidentiality, non-repudiation, integrity, cipher text authenticity, & open verifiability	The access control scheme for authorizing, authenticating, and revoking users to use WBAN was created based on the sign encryption scheme	Identity-based cryptography is missing and has Undergone from larger consumption of computational power
17	ACP achieved the node authentication as well as delivered identity privacy for the communicating entities such as source, destination & intermediate nodes.	To prevent malevolent nodes from eavesdropping on the network and to secure the node's privacy, an ECC-based Access Control Protocol (ACP) solution was proposed.	The data integrity.
20	They allowed Internet users in a certificate-less cryptography environment to communicate along a sensor node in an identity-based cryptography environment along different system parameters.	Provides Resists Physical Device Capture, provides key Agreement, Resists Device Impersonation, and Resists Malicious Device Deployment	Mutual authentication and anonymity
21	A unique physical layer security transmission mechanism based on the Alamouti Space-Time Block Coded Non-orthogonal Multiple Access (STBC-NOMA) scheme.	Research goals are mainly focused on wiretap channel	Multi transit antenna
22	a heterogeneous signcryption scheme for WBANs based on an identity-based cryptosystem (IBC) and a public key infrastructure (PKI) with an equality test (HSCIP-ET).	Suggested a heterogeneous solution for WBAN that rely on an equality test to migrate from identity-based to public key infrastructure	For security complexity, use bilinear pairing, which is a computationally demanding technique.

In [23] a novel hyperelliptic curve-based architecture for WBANs known as the secure channel free certificates signcryption approach was introduced. On the other hand, the authors were unable to satisfy any of the claim security criteria with any type of formal or informal proof. In [24] Data anonymization methods and differential privacy have been widely implemented in medical and healthcare research domains to safeguard privacy while exchanging e-health data. In [25] uses adaptive physiological monitoring and rescue system to rescue data and classification of packets.

2.3. Research Gaps

From the above literature, we have highlighted the key research gaps in this work:

- For IoT-enabled health services, security is a big problem. Trust-based systems monitor the activity of IoT nodes and prevent hostile nodes from being involved in medical data transfer, however, such solutions fall short of addressing data security and privacy concerns. Concerns about confidentiality and protection
- The cryptography-based mechanisms lead to the excessive burden of resource utilization to achieve data security and privacy.
- Recent security & privacy preservation solutions using ECC for healthcare systems are just at the beginning level.
- There is a lack of exploration through considering the various properties & other challenges like mobility, energy efficiency, real-time computing, etc. of WBANs while designing the security solutions or access control policies.

2.4. Summary

As per the literature and research gaps mentioned in this chapter, it needs an effective cryptography-based method that achieves the security and privacy of medical data and users in IoHT with minimum energy consumption and overhead. The ECC provides strong security with minimum space and time requirements. It motivates us to present the novel SEECC protocol for IoHT.

3. LIGHTWEIGHT ACCESS CONTROL POLICIES

The goal of the proposed protocol is to achieve lightweight medical data security and privacy preservation effectively without compromising the network QoS performance. For that reason, we have used the ECC-based cryptography technique. Before presenting the ECC with the ECDSA mechanism of secure medical data transmission approach, we

RESEARCH ARTICLE

present the functionality of ECC and its role in wireless networks.

3.1. Functionality of ECC

Many cryptography algorithms rely heavily on modular multiplications [26]. ECC is a newer trend in application development than previous encryption technologies. ECC is a public key cryptography encryption technique that uses the algebraic format of an elliptic curve with finite fields. The revealed ECC uses the basic Galois field to guarantee security while transmitting data from one point to another. Pseudorandom number generators, key agreements, and digital signatures are all examples of applications that use the secure ECC-based transaction process [27]. Because of its low storage requirements, effective transmission requirements, and lower key size, elliptic curve cryptography has been widely used in numerous secure transactions [28]. In general, ECC ensures high-level security; if the approach uses a 256-bit public key, it is safer than 3072-bit RSA public key security.

ECC algorithm consists of an elliptic curve along with the finite field while performing the cryptographic process defined as follows, [29]

$$E: y2 = x3 + ax + b \quad (1)$$

Equation (1) denotes the plain curve of the elliptic curve where 'E' defines the elliptic curve, 'a' and 'b' are the integers or rational numbers, and 'x', and 'y' can be any rational numbers in the elliptic curve. The defined elliptic curve has been operated in the Abelian group which is derived from the divisor group which is defined as follows. The Picard group of E which is denoted as Pic (E) as defined in Equation (2):

$$Div \rightarrow Pic(E) \quad (2)$$

Quotient out by linear equivalence is shown in Equation (3)

$$Div \rightarrow Pic(E) \cong E \quad (3)$$

As shown in Equation (3) where Div E is the group of divisors on E of degree 0. The Picard group of E which is denoted as Pic (E) and according to the inherited elliptic group values is used while making the transaction. The elliptic algorithm utilizes the elliptic curve point multiplication process while performing the cryptographic process. Elliptic curve point multiplication is the process of adding the point value along with the elliptic curve continuously for ensuring the security of information. This point of multiplication is called scalar multiplication which is called the Hessian Elliptic Curve (HEC). Let the 'E' elliptic curve includes a few finite fields that are defined by Equation (1). For this elliptic curve, point multiplication is denoted as follows,

$$nP = P + P + P + \ldots\ldots + P \quad (4)$$

In Equation (4), 'n' is the scalar integer value, and 'P' lies on the curve 'E' which is commonly called the Weiestrass curve. The Logarithmic Problem (LP) can be determined using the 'n' value in the curve and LP occurs if it is larger than the Q and P values of the curve. So, the point of addition or multipliers must be considered for eliminating the discrete logarithm problem. According to the discussions, the significance of this research is to optimize ECC architecture through different multipliers for managing the security, area overhead, on-chip power, utilization of memory, and delay in an efficient manner.

3.2. Finite Field Multipliers

The finite field is also called the arithmetic field which includes finite and infinite numbers for performing a particular process. Generally, the finite field is represented in the form of **p** in which 'n' is represented as the positive integer and 'p' is the prime number. When the two finite fields have the same size commonly called an isomorphic issue. When 'p' is the characteristic of the field and 'n' is the dimension of the prime field. According to the finite field discussions, different multipliers chosen are point addition, point doubling, polynomial multipliers, etc.

3.2.1. Point Addition

The Point addition process consists of two negation points such as 'P' and 'Q' which intersect the curve 'E'. So, the line as shown in Equation (5):

$$P + Q = R \quad (5)$$

$$x, yx, y = (x, y) \quad (6)$$

For the two negation points such as 'P' and 'Q' and the resultant 'R' are shown in Equation (6), The elliptic curve over real numbers is defined as the set of points (x,y), then the elliptic curve has been defined in Equation (7):

$$\lambda = \frac{y_q - y_p}{x_q - x_p} \quad (7)$$

Where 'λ ' represents the slope of the line through 'P' and 'Q' as sown in Equation (8):

$$xr = \lambda 2 - xp - xq \quad (8)$$

$$y_r = \lambda(x_p - x_r) - y_p \quad (9)$$

3.2.2. Point Doubling

The other multiplier is point doubling in which 'P' and 'Q' points are co-incident. The defined points are expressed in terms of a closed limiting case. So, the curve is defined as follows in Equation (10):

$$\lambda = \frac{3x_p^2 + a}{2y_p} \quad (10)$$

RESEARCH ARTICLE

In Equation (10), 'a' is the real number denoted from the elliptic curve 'E'.

3.2.3. Polynomial Multiplier

The straightforward multiplier is called the polynomial multiplier which is defined as Galois Field (GF (2)). Consider A(x) and B(x) as two polynomial functions ranging from k=0, m-1, the output of the multiplication is C(x) with degree-bound k=0, 2m-1. Then the polynomial coefficients are represented as follows:

$$C_k = \begin{cases} \sum_{1=0}^{k} a_1 b_{k-1} & \text{for } k = 0, \ldots m-1 \\ \sum_{i=k}^{2m-2} a_{k-1+(m-1)} b_{i-(m-1)} & \text{for } k = m..2m-2 \end{cases} \quad (11)$$

As shown in Equation (11) degree-bound of 'C' is the sum of the degree-bounds of 'A' and 'B', if a polynomial has degree-bound 'k', it also has degree-bound k + 1. Further 'a' and 'b' are the coefficients of A(x) and B(x), where 'x' defines the given point on the polynomial function (Parrilla *et al.* 2018). During this process, the Karatsuba multiplication is used to develop the polynomial multiplication. Consider if the multiplication process utilizes 192 polynomial degrees which are developed in terms of applying the iterative steps that use the multiplier (degree 64) six times. The input functions 'A' and 'B', denoted as 'R' in Equation (12):

$$R = A.B \text{ where } A = \sum_{i<deg(A)} \sum_{j<deg(B)} (a_i \oplus b^j) x^{i+1}$$

$$= (a_0 b_0)(x^0 \oplus x^{2n}) \oplus (a_1 b_1)(x^{2n} \oplus x^{3n})\ (a_2 b_2)(x^{3n} \oplus x^{4n})$$
$$(a_2 \oplus a_0)(b^2 \oplus b^0)(x^n \oplus x^{2n})\ (a_2 \oplus a_1)(b_2 \oplus b_1)(x^n \oplus x^{3n})(a_2 \oplus a_1 a_0)$$
$$(b_2 \oplus b_1 \oplus b_0) \quad (12)$$

Then the linear squaring property is applied on the 192 degrees of polynomial multiplication as follows in Equation (13):

$$R = A.A = a_0^2 x^0 \oplus a_1^2 x^{2n} \oplus a_2^2 x^{4n} \quad (13)$$

This polynomial multiplication process needs an additional reduction step while performing the field multiplication process. In addition to this, the field polynomial multiplication process works efficiently by utilizing the XOR operation and shifting algorithm. Moreover, the polynomial multiplication process has been implemented in a standard ECC curve based on the identities which are more applicable to any kind of trinomial 'T' that is represented as follows in Equation (14):

$$T = R \bmod (x^n + x^m + 1) = r_{0_{n-1}} \oplus (r_{n \ldots \deg(R)} \oplus (x^m + 1)) \quad (14)$$

The polynomial multiplication process applicable to different trinomials, still work very slowly and becomes challenging while implementing security. Based on the working process of multipliers in the finite field over an elliptic curve, need to ensure security in different applications such as digital transactions, WBAN, WSN, key generators, Vehicular Ad hoc Networks (VANET), biomedical applications, etc. Among the various applications, WSN and WBANs are one of the most effective fields because it used to transmit information in real-time scenarios.

3.3. Montgomery Multiplier

[30] Modular multiplication (Z) of two numbers 'a' and 'b' is defined as shown in Equation (15):

$$Z = a * b \ (\text{Mod } p) \quad (15)$$

The Montgomery multiplication operates on Montgomery residues (and b**)** can be computed and shown in the Equation (16) and (17):

$$\check{a} = a * r \bmod p \quad (16)$$

$$\check{b} = b * r \bmod p \quad (17)$$

The Montgomery duplication strategy needs 'r' and 'p' to be moderately prime. This can be accomplished by taking odd numbers for 'p', while 'r' is picked as a force of 2. Galois field Gf(p) method of activity, r^2 mod p esteem is a contribution from the UI, while for Gf(2^n) method of activity, the coefficients of r^2 (x) mod p(x) are a contribution from the UI:

$$RR^{-1} = 1 (\bmod p) \quad (18)$$

$$z = zr = abr(ar * br)r^{-1} = zr^{-1} \bmod p \quad (19)$$

$$zr^{-1} \bmod p \quad (20)$$

$$z = a * b (\bmod p) \quad (21)$$

As shown the Equation (18), the Montgomery augmentation calculation gives an r^{-1} to the outcome. Because of this, the calculation is not straight fitting to enter operands. The Montgomery duplication is characterized as; all components should be changed to the Montgomery build-up field. As shown the Equation (19) Montgomery build-up Z field is handled to address the r–increased upsides of the operands, as a•r and b•r. The operands a and b are indivisible number field components or twofold expansion field components. At that point, the change tasks are applied to the two operands an and b, before the duplication and to the moderate outcome 'c' to get the end-product Z as demonstrated in the Equation (20 and 21) Montgomery increase will not be performed for a solitary secluded augmentation. It is more proficient for exponentiations and the numbers are duplicated commonly. The benefit of Montgomery increase is unmistakably apparent, as in ordinary secluded augmentation number division is required.

3.4. Role of ECC in WSN/WBAN

WSN/WBAN consists of an enormous quantity of sensor nodes that are capable to transmit a message from one location to another location [31]. In WSN/WBAN many

RESEARCH ARTICLE

nodes are deployed to monitor a wide variety of applications such as security monitoring in military applications, environment monitoring, and other remote places monitoring, etc. The network consists of a collection of nodes which is interconnected to each other for making an effective transmission of information. Security is one of the challenges in the network due to several intermediate attacks present in the sensor networks [32]. For managing these security challenges, the symmetric algorithm is applied to the network which maintains the network energy used to maximize the network lifetime in turn improves the network confidentiality. As a result, the ECC cryptosystem technique is utilised to assure security, secrecy, and authentication for managing security by leveraging effective network resources. In addition to this, the ECC has been used to improve energy conservation as well as manage the key effectively while transmitting the data in the sensor networks. Along with this, the ECC algorithm effectively manages the key distribution and storage issue by performing the secret key settings. Then the sample key size comparison of ECC with other algorithms is shown in Table 2. Table 2 indicates that the ECC algorithm ensures long-term security while using a smaller size key when compared to the other encryption algorithms. So, the ECC algorithm has been used to maintain the security between the nodes in WSN. The elliptic curve consists of finite field 'Fp' which performs the encryption and decryption process by using the point G and elliptic group of parameters such as $E_{qu}(a,b)$.

Table 2 Key Size Comparison

DSA Key size	RSA Key size	ECC Key size	Key size Ratio	Comment
512	1024	160	1:6	Security of Short period
2048	3072	256	1:12	Security of Medium period
3072	7680	384	1:20	Security of Long term

Then the ECC-based encryption must be performed while transmitting the message from sender 'A' to receiver 'B'. During the encryption process, 'A' selects the random number 'k' and creates the cipher text 'Cm' which is explained as follows:

$$Cm = [k * G, Pm + k * P_B] \quad (22)$$

In Equation (22) 'Cm' is represented as the cipher text, 'k' is the random positive integer, Pm is the transmitted message, and at the time of transaction 'A' utilizes the 'B's public key which is denoted as the P. After receiving the cipher text, the receiver performs the decryption process which is done by the multiplication and subtraction process. The receiver 'B' utilizes the private key 'n_B' and subtracts the obtained result from the second point which is done as shown in Equation (23).

$$p_m + k * p_B - n_B(k * G) = p_m + k(n_B * G) - n_B(k * G) = p_m \quad (23)$$

Depending on the decryption process, the 'A' and 'B' related key exchange process has been defined as follows:

- Initially, sender A selects A's private key when $n_A < n$
- Sender A generates the public key when $P_B = n_{B-G}$ where, the point Eq. (a,b)
- Receiver B selects B's private key when $n_g < n$
- Receiver B generates the public key $P_B = n_{B-G}$ where point Eq. (a,b)
- After that, the defined public keys are exchanged between A and B, then generate the secret key of 'A' is Na*P_B. B's secret key is n_8*P_A.

The elliptic curve cryptology algorithm, dependent on the preceding method, sends the message from sender to receiver while assuring security, secrecy, and integrity, as well as managing the key. Due to the effective key management and security process, ECC has played an important role in WSN/WBAN. The Montgomery multiplication design process was applied to the hardware dataflow of the ECC algorithm to improve the data transmission process.

3.5. Importance of Finite Field Multipliers and Montgomery Multipliers in WSN/WBAN

The efficiency with which arithmetic operations are realized in the underlying finite field determines ECC performance. [33].

Modular addition in GF(2m) is straightforward. Therefore, it may be constructed using only XOR gates. Because only one inversion operation is required after the scalar multiplication when utilizing projective coordinates for ECC, the inversion cost may be neglected. The modular squaring in GF(2m) is simple. [34]. As a result, the most significant operation in ECC implementations is modular multiplication.

The Montgomery modular multiplication algorithm is widely used as an efficient algorithm [35].

4. PROPOSED MODEL

4.1. System Design

Figure 1 [36] demonstrates the design of an intelligent smart healthcare system The periodic patient data collected at each IoT node is transmitted to local access point nodes. Finally, the data collected at access point nodes is transmitted to the

RESEARCH ARTICLE

central medical gateway node where the medical experts access the patient's data and do the analysis and decision-making processes. The data transmissions among IoT nodes and IoT nodes to access points have been performed by wireless interfaces. For this model, we used the 802.15.4 (Zigbee) interface. The reason for selecting the 802.15.4 MAC layer standard as it is more suitable for WBAN communications by considering the interference management among various IoT nodes in WBANs. Furthermore, this standard is considered very close to WBAN because of its reliable in-built security approach as well as the support of low data rate applications with low cost of power consumption. During the experimentation, we configured each WBAN node with this standard so that they adopt the 802.15.4 functionality. The proposed system design also considers the malicious IoT nodes in the network that perform malicious activities in communications so that data drop, network delay, and overhead problems arise.

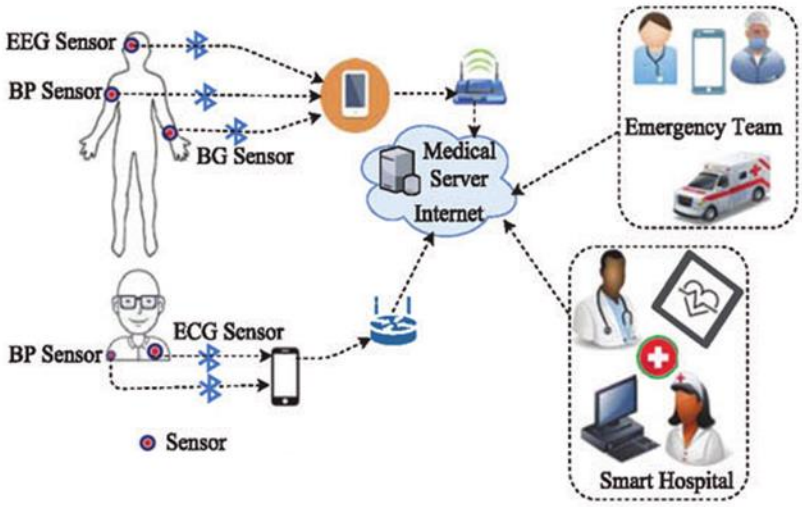

Figure 1 WBAN-Assisted Smart Healthcare System

4.2. Assumptions

The system design presented in Figure 2 is having some assumptions for the simulation and analysis purpose such as:

- The network for representing the smart healthcare system consists of WBAN (IoT) nodes, access point nodes, and gateway nodes.
- Each IoT node consists of 4 different body sensors.
- These four body sensors in each IoT node collect periodic medical data and transmit it locally at the local processing unit. The four body sensors are a temperature sensor, Electrocardiography (ECG) sensor, Pulse Oximeter (PO) sensor, and a Blood Pressure (BP) sensor. We assumed that the ECG sensor was placed at the chest of the human body, the BP sensor placed on the right lower shoulder, the PO sensor placed near the right-hand thumb, and the temperature sensor placed at the right-hand forearm of each human body.
- The data collected at the local processing unit of each IoT node is further transmitted periodically to the near access point node using routing functions.
- We assume that all IoT nodes are homogenous, energy-constrained, and static with a unique ID.
- The communication among sensor nodes is multi-hop symmetric communication.

The network consists of attackers in the network which are 10 % of the total IoT nodes in the network. It is called a malicious attacker as they attract all data packets by fake Route Response Packet (RREP) to dishonestly pretend a new and shortest route to the destination and then drop them without forwarding them to the destination.

4.3. Proposed Algorithm

The proposed solution consists of a smart healthcare system using WBAN-assisted IoT in the presence of malicious nodes in the network. The proposed model is tested against the performance of two access control protocols such as ACP [17] and CDHSC [20]. Figure 2 shows the model of the proposed algorithm. When attempting to provide a solution in IoT WBAN, we first install sensing devices and various components depending on the situation for which we are looking for a solution following installation, fully distributed management will ensure that all sensors and nodes are operational. According to [37], the fundamental focus of WBAN is cost and energy savings. After route discovery, the lightweight secure communication-based ECC was implemented as per algorithm 1.

RESEARCH ARTICLE

The approach uses the authentication and authorization methods proposed to achieve lightweight secure data transmission. For the WSN data transmission procedure, the ECC technique is created utilizing the Elliptic Curve Digital Signature Algorithm (ECDSA). Algorithm 1 demonstrates how the suggested algorithm works in the privacy-preserving cryptography-based method as secure communication-based ECC (SCECC).

Using the mathematics of elliptic curves, ECC ensures security among key pairs. A similar concept was used in RSA, except instead of elliptic curves, prime integers were used. Because of its high security and minimal key sizes, ECC has received a lot of attention. Because ECC relies on the shape of elliptic curves for public-key cryptography operations, its keys are extremely difficult to crack. Because of the security and computational efficiency of ECC, we established access control rules in the algorithm to transfer medical data from IoHT users to specified access points. This algorithm not only secures data but also protects the privacy of users.

The function $[P^1, P^2] = getEccKeys()$ generates the public (P^2) using an elliptic curve of 128-bit and private (P^1) keys randomly. The $hybridCrypto()$ function performs the hybrid cryptography of input medical data P. As no direct encryption/decryption is provided by ECC, hybrid encryption/decryption is proposed by utilizing the key exchange protocol called Elliptic Curve Diffie-Hellman (ECDH). ECDH is used to provide the shared secret key for symmetric message encryption/decryption. This ensures strong data security against various cyber threats with the minimum overhead of key sizes. For authentication purposes, we generate the digital signature of encrypted messages using a lightweight ECDSA technique. The signature is verified at each intermediate and destination node to verify message integrity.

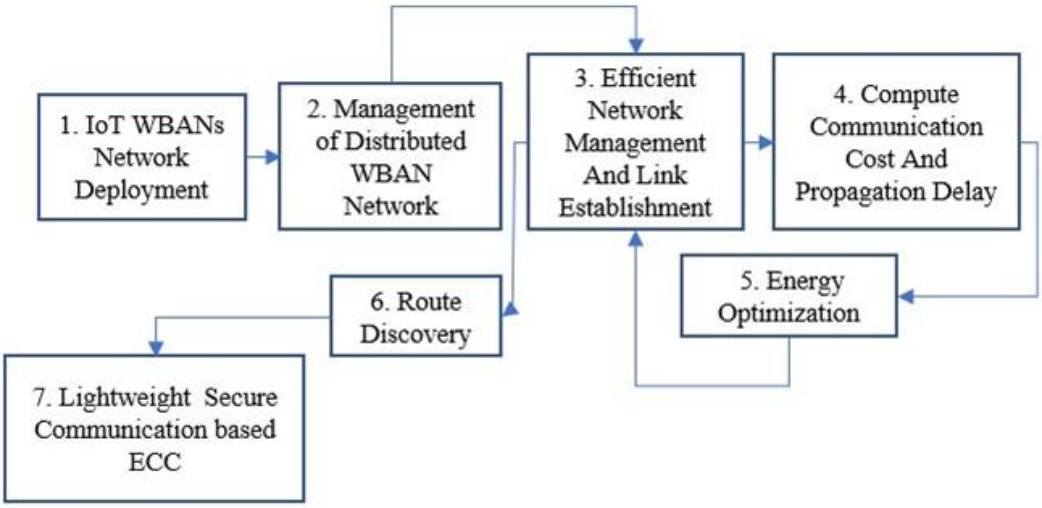

Figure 2 Proposed Algorithm

Inputs
I: *Source IoHT Node*
AP: *Intended Acess Point*
P: *Input medical data*
Output
Secure data transmission

1. Source Node
   - 1.1. $[P^1, P^2] = getEccKeys()$
   - 1.2. $P^{encrypt} = hybridCrypto(P, P^2, 'encrypt')$
   - 1.3. Node S sign packet P using public and private keys generated:
   - 1.4. $P^{hash} = SHA2(P^{encrypt})$
   - 1.5. $P_{sign}^{encrypt} = ecdsa\ (P^{hash}, P^1, P^2)$
   - 1.6. Forward $(P_{sign}^{encrypt},\ next - hop)$
2. Relay Node
   - 2.1. If $(next - hop \neq AP)$
   - 2.2. Verify the P^2 validity
   - 2.3. $P^{hash} = SHA2(P^{encrypt})$
   - 2.4. Compute the curve points P^2
   - 2.5. $f = verify\ (P^{hash}, P^1, P^2)$
   - 2.6. If $(f\ == 1)$
   - 2.7. $P_{sign}^{encrypt} = ecdsa\ (P^{hash}, P^1, P^2)$
   - 2.8. Forward $(P_{sign}^{encrypt},\ next - hop)$

RESEARCH ARTICLE

2.9. Else

2.10. discard ($P^{encrypt}$)

2.11. End If

2.12. Else

2.13. Go to Step 3

2.14. End If

3. Access Point Node

3.1. Verify the P^2 validity

3.2. $P^{hash} = SHA2(P^{encrypt})$

3.3. Compute the curve points P^2

3.4. $f = verify\ (P^{hash}, P^1, P^2)$

3.5. If ($f\ == 1$)

3.6. $P^{decrypt} = hybridCrypto(P^{encrypt}, P^2, decrypt')$

3.7. Else

3.8. discard ($P^{encrypt}$)

3.9. End If

4. Return acknowledgment of successful packet delivery

Algorithm 1 Secure WBANs Communication (SCECC)

5. RESULTS AND DISCUSSIONS

This section presents the simulation environment of a smart healthcare system using WBAN-assisted IoT networks.

5.1. Simulation Environment

Several simulators like OPNET, Qualnet, and NS2 are available to mimic networks such as mobile ad hoc networks known as WSNs or WBANS. We used NS2 in this project. NS2 is frequently used for all protocols, including commonly used IP protocols over both wireless and wired networks. In comparison to wireless simulation, which is only partially supported by NAM, wired network simulation is completely supported. the properties of the ns-2 pique our curiosity in utilizing it to simulate our network applications, including:

- NS2 provides the network reproduction environment for both wired and wireless MANET networks.
- Specifies the set of routing rules for the choice into whatever networking is done in various methods.

NS2 is an object-oriented network simulator built with technologies such as CPP and OTCL. Table 3 compares the availability, programming language support, and other features of these three network simulators based on what we learned from studying them.

Table 3 Comparison of the Network Simulators

Simulator	Free	Open Source	Programming Language
NS-2	Yes	Yes	C++.TCL
GloMoSim	Limited	Yes	Parse
Opnet	No	No	C

5.2. Threat Model

To consider the smart healthcare applications, we introduced the malicious node conditions in WBANs. We believed that any sensor node in WBAN may become malicious due to several reasons. The sensor node attacker conditions in the network are assumed as the malicious node attack that leads too many packet failures in the system. The problem of runtime malicious attacks becomes very harmful to the entire WBAN communication protocol. This creates significant challenges in securing medical data and privacy preservations. Therefore, lightweight methods are required to protect from these attackers. The network consists of malicious attackers that are 10 % of the total IoHT nodes in the network. It is an active attack that drops the data packets in the network intentionally. It is called a malicious attacker as they attract all data packets by fake Route Response Packet (RREP) to dishonestly pretend a new and shortest route to the destination and then drop them without forwarding them to the destination.

5.3. Visualization Results

In this section, we present the results of NAM. NAM is a Tcl/TK based network. It upholds geography design and different information investigation devices. NAM started at LBL. It has developed considerably in recent years. The NAM improvement exertion was progressing cooperation with the VINT project.

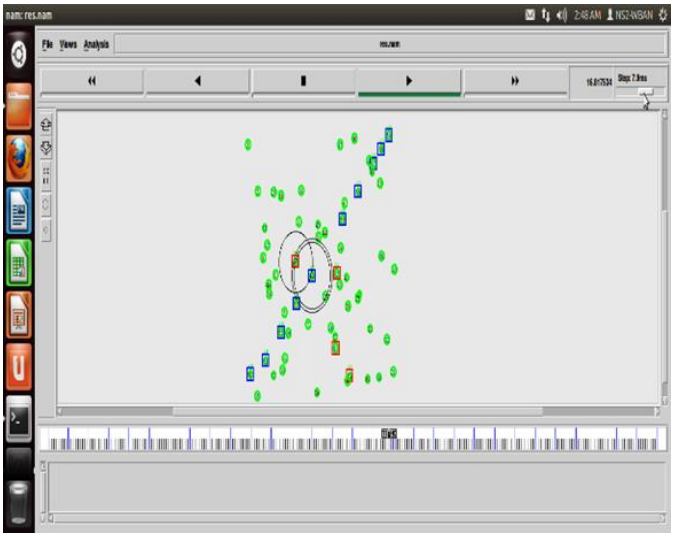

Figure 3 Data transmission Among the Source and Sink Pairs

RESEARCH ARTICLE

Figure 3 shows that the different sensor nodes periodically transmit the data towards the intended sink nodes via the Aps, where the access points are colored blue and the sensor nodes are colored green. WBANs and access points are found randomly among all nodes (APs). The green hue indicates that the nodes' batteries were fully charged before the simulation started. The NAM results do not give us the performance of the simulated network; therefore, we must use the trace files to measure the various performance metrics.

Figure 4 demonstrates the WBANs communications in presence of the malicious attackers, Attacker node's presence was signaled by the color red. The scenario is focused on reliability evaluation by varying the number of malicious nodes in the network from 0 to 20 % of total IoHT users.

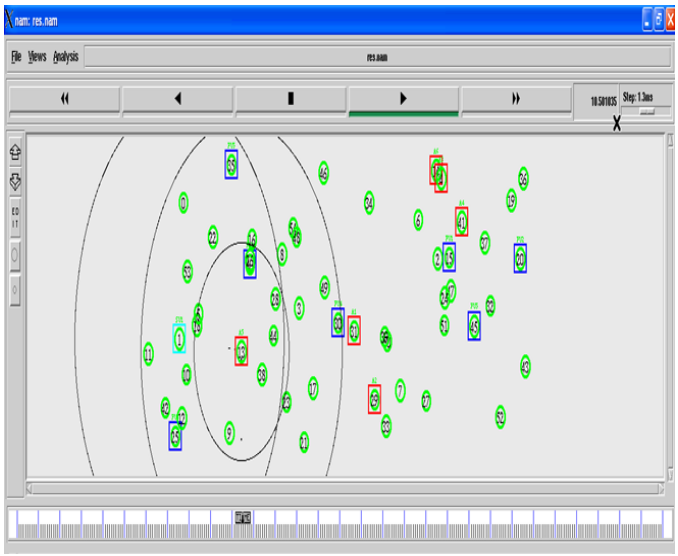

Figure 4 Network Data Communications in Presence of Malicious Nodes

5.4. Performance Metrics

The implementation & evaluation of these protocols were performed using NS2. The networks are designed using the parameters shown in Table 4. The Number of WBANs is varying from 25 to 150 to consider the small to large networks for the evaluations of ACP and CDHSC protocol.

Table 4 Simulation Parameters for Attacker Variations

Parameters	Values
Area of Network	1000 x 1000
Network Type	WBAN
Number of WBANs	25-150
Velocity	2 m/s
Time of Simulation	50 sec
Initial Energy	0.5 J
Consumption of Transmitter energy	16.7 nJ
Consumption of Receiver energy	36.1 nJ
Attackers	10 %
Security Solutions	ACP & CDHSC
Malicious IoHT users	0/5/10/15/20 %

The mobility speed of each WBAN node is considered a maximum of 2 m/s as a normal human being is moving with this speed maximum. The other parameters and their values were selected as the standard model for the evaluations. The data traffic among the WBAN nodes is considered as the Constant Bit Rate (CBR) format as the numerical values are sensed by the four sensors (temperature, BP, PO, and ECG sensors) periodically. These numeric values are transmitted to the central gateway node in form of CBR only. The data transmission rate is 2Mbps with a packet size of 512 Kbytes.

5.4.1. Average Delay

This metric computes the average time under packet origination time at every source & packet forwarding time at all destination nodes. It is computed as shown in equation (24): [38]

$$D = \frac{\sum_{i=1}^{N}\left(d_t^i + d_p^i + d_{pc}^i + d_q^i\right)}{N} \qquad (24)$$

Where N denotes the number of transmission links, d_t^i is the transmission delay of i^{th}link, d_p^i is the propagation delay of i^{th}link, d_{pc}^i is the processing delay of i^{th}link, & d_q^i is queuing delay of i^{th}link.

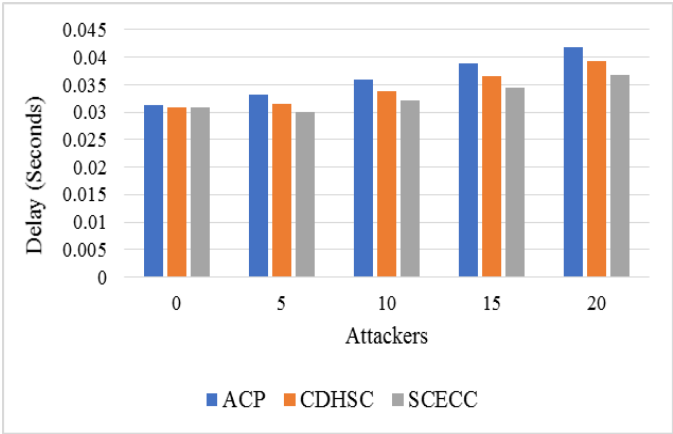

Figure 5 Average End-to-End Delay Analysis for Attacker Variations

Table 5 Average Delay Readings in Attacker's Variation

	ACP	CDHSC	ECEBA
0	0.03119	0.03092	0.03083
5	0.03328	0.03156	0.03
10	0.0359	0.0339	0.03211
15	0.03896	0.03662	0.03454
20	0.04172	0.03926	0.03687

RESEARCH ARTICLE

The average delay (Figure 5 and Table 5) should be lower for the efficient privacy-preserving protocol.

5.4.2. Average Throughput

This kind of metric computed the number of packets delivered every second. The average throughput under Kbps is as per the equation (25): [39]

$$T = \left(\frac{R}{T^2 - T^1}\right) \times \left(\frac{8}{1000}\right) \quad (25)$$

Where R has completely received packets at every destination node, T^2 has been stop time of simulation & T^1 start time of simulation.

The throughput results in Figure 6 and Table 6 show that WBAN increases and throughput decreases. This is due to an increasing number of interconnections among the IoT nodes for data transmissions. The throughput needs to be higher for the efficient privacy-preserving protocol.

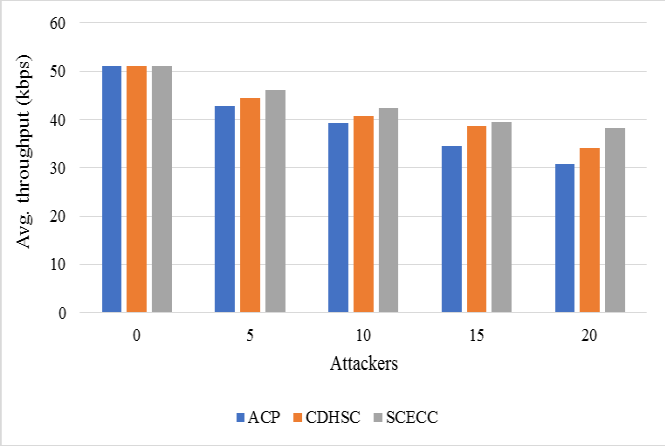

Figure 6 Average Throughput Analysis for Attacker Variations

Table 6 Readings of Average Throughput for Attacker's Variation

	ACP	CDHSC	ECEBA
0	51.15	51.15	51.15
5	42.74	44.35	46.09
10	39.37	40.82	42.46
15	34.55	38.57	39.5
20	30.85	34.09	38.15

5.4.3. Average Energy Consumption

It has been calculated the consumption of average energy through the available network after the simulation end by counting the reduction of available energy of every node. Total energy consumed E^{tot} has been calculated as shown in equation (26): [39]

$$E^{tot} = \sum_{i=1}^{N} \left(E_i^{initial} - E_i^{consumed}\right) \quad (26)$$

Where $E_i^{initial}$ & $E_i^{consumed}$ was basic & consumed energy of i^{th} node respectively. N has been an overall number of nodes under the network. Average consumed energy has been calculated as per equation (27):

$$E^{avg} = \frac{E^{tot}}{N} \quad (27)$$

Figure 7 and Table 7 demonstrate the average energy consumption performance of the three protocols. As per observations, the performance using CDHSC is worst for energy efficiency compared to ACP and SCECC.

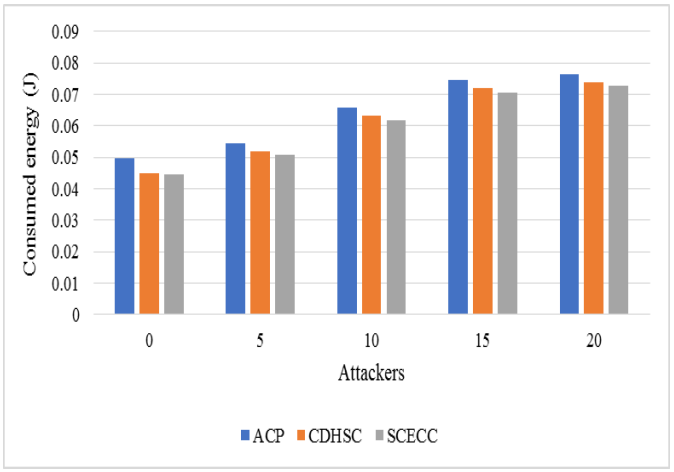

Figure 7 Average Energy Consumed Analysis for Attacker Variations

Table 7 Readings of Average Energy Consumption in Attacker's Variation

	ACP	CDHSC	ECEBA
0	0.0496	0.04504	0.0446
5	0.05455	0.05205	0.05085
10	0.06565	0.06315	0.06195
15	0.07445	0.07195	0.07075
20	0.076455	0.07395	0.07275

5.4.4. Packet Delivery Ratio (PDR)

It has been the computation of the ratio of the packet received through destinations that were forwarded through different resources of various traffic patterns. It is calculated as shown in equation (28): [38]

$$P = \left(\frac{P_r}{P_g}\right) \times 100 \quad (28)$$

Where, P_r have been several received packets & P_g a number of generated packets.

RESEARCH ARTICLE

The dropped packets are computed as shown in equation (29):

$$Drop = P_g - P_r \quad (29)$$

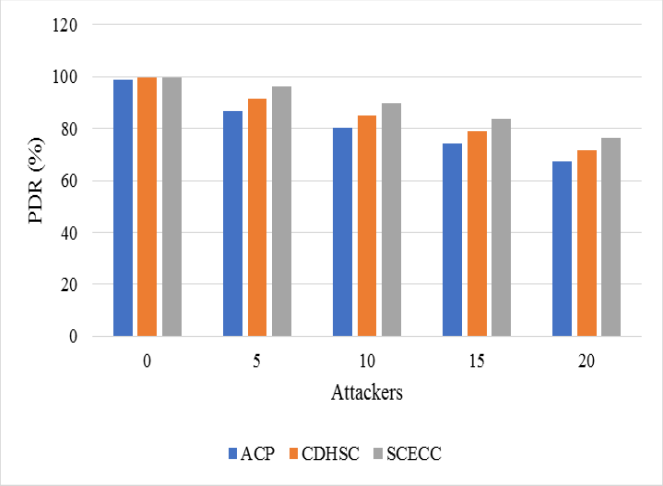

Figure 8 PDR Analysis for Attacker Variations

Table 8 Readings of PDR in Attacker's Variation

	ACP	CDHSC	ECEBA
0	99.051	99.68	99.89
5	86.81	91.56	96.3
10	80.48	85.23	89.97
15	74.156	78.9	83.64
20	67.37	71.59	76.24

The PDR (Figure 8 and Table 8) results demonstrate a similar trend as throughput results.

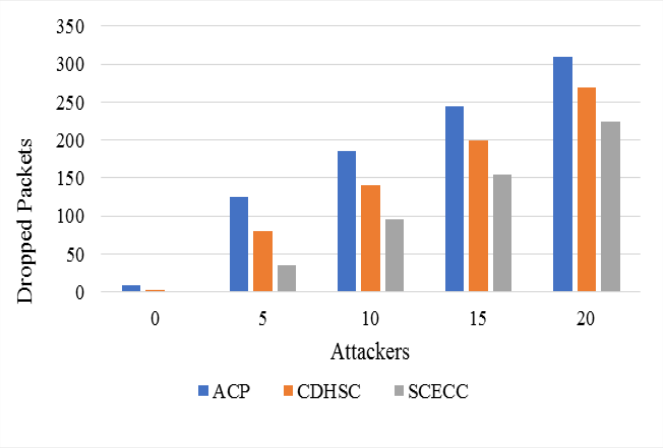

Figure 9 Number of Dropped Packets Analysis for Attacker Variations

The number of packets dropped (Figure 9 and Table 9). The QoS parameters PDR and throughput are required to be higher whereas the parameters delay and packet drop should be lower for the efficient privacy-preserving protocol.

Table 9 Total Dropped Packets in the Attacker's Variation

	ACP	CDHSC	ECEBA
0	9	3	1
5	125	80	35
10	185	140	95
15	245	200	155
20	309	269	225

5.4.5. Communication Overhead

It has been calculated as a ratio of the total number of routing packets to the total number of data packets under the network. It is computed as shown in equation (30) : [38]

$$O = \sum_t \left(\frac{RT^t}{DT^t}\right) \quad (30)$$

Where, RT^t is the total number of routing packets & DT^t is the total number of data packets at time t.

The computation burden on IoT nodes is higher using ACP and CDHSC compared to SCECC (Figure 10 and Table 10). The SCECC uses the digital signature of encrypted messages using a lightweight ECDSA technique. The signature is verified at each intermediate and destination node to verify message integrity which takes less computational burden than ACP and CDHSC security operations.

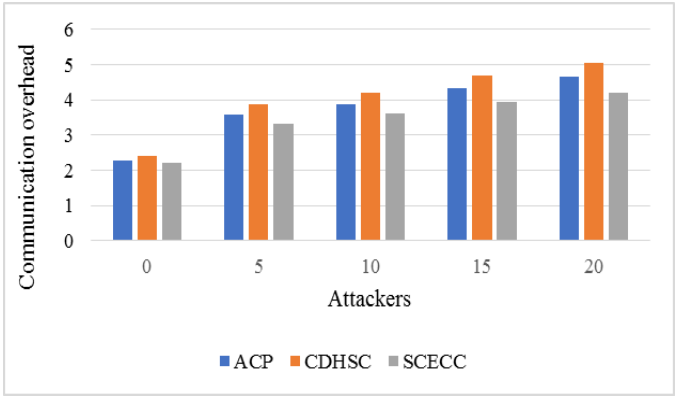

Figure 10 Communication Overhead Analysis for Attacker Variations

These results indicate the QoS performance of WBANs in the presence of attackers. The increasing number of attackers leads to a negative impact on the performance of all protocols. In ACP more focus is on node privacy, however, protecting the data is solved by the SCECC algorithm. The SCECC addresses the privacy preservation and security of communications effectively in presence of malicious attackers in our simulation outcomes.

RESEARCH ARTICLE

Among three protocols simulated ACP, CDHSC, and SCECC, the latter shows the improvement in all QoS parameters, due to the digital signature of encrypted messages using the lightweight ECDSA technique. The signature is verified at each intermediate and destination node to verify message integrity.

Table 10 Communication Overhead Readings in Attacker's Variation

	ACP	CDHSC	ECEBA
0	2.28	2.395	2.227
5	3.588	3.881	3.337
10	3.89	4.207	3.617
15	4.342	4.697	3.928
20	4.669	5.066	4.208

6. CONCLUSION

The ACP protocol is a lightweight approach for WSN that addressed the privacy of node identity using ECC, crypto system, and hash function. On other hand, the CDHSC protocol designed for IoT enabled WBAN that achieved stronger security with minimum computation efforts. For real smart healthcare systems using the WBAN-assisted IoT, the mechanism required for privacy preservation & trustworthy cooperation among nodes to communicate personnel medical information. To satisfy the trade-off between minimum resource utilization & higher security/privacy performance, the proposed SCECC access control schemes are being implemented & evaluated using the NS2 along varying WBANs size in the presence of malicious attackers. The simulation results were measured in terms of average throughput, PDR, packets dropped, average delay, average energy consumption, & communication overhead. The results show that SCECC privacy-preserving method achieved the trade-off between the energy-efficiency & security efficiency. For future work, we suggest simulating the different attack scenarios to achieve the trade-off in performances through dynamic node allocation with energy & cost management along an access control scheme.

REFERENCES

[1] P. Gope & T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network", IEEE Sensors J., vol. 16, no. 5, pp. 1368-1376, May 2016.

[2] C. C. Poon, B. P. Lo, M. R. Yuce, A. Alomainy & Y. Hao, "Body sensor networks: In the era of big data & beyond", IEEE Rev. Biomed. Eng., vol. 8, no. 1, pp. 4-16, Apr. 2015.

[3] T. Wu, F. Wu, J. Redouté & M. R. Yuce, "An Autonomous Wireless Body Area Network Implementation Towards IoT Connected Healthcare Applications," in IEEE Access, vol. 5, pp. 11413-11422, 2017, doi: 10.1109/ACCESS.2017.2716344.

[4] Mahajan, H. B., & Badarla, A. (2018). Application of Internet of Things for Smart Precision Farming: Solutions & Challenges. International Journal of Advanced Science & Technology, Vol. Dec. 2018, PP. 37-45.

[5] Mahajan, H. B., & Badarla, A. (2019). Experimental Analysis of Recent Clustering Algorithms for Wireless Sensor Network: Application of IoT based Smart Precision Farming. Jour of Adv Research in Dynamical & Control Systems, Vol. 11, No. 9. 10.5373/JARDCS/V11I9/20193162.

[6] Javadi S.S., Razzaque M.A. (2013) Security & Privacy in Wireless Body Area Networks for Health Care Applications. In: Khan S., Khan Pathan AS. (eds) Wireless Networks & Security. Signals & Communication Technology. Springer, Berlin, Heidelberg.

[7] Amutha, J., Sharma, S. & Nagar, J. WSN Strategies Based on Sensors, Deployment, Sensing Models, Coverage & Energy Efficiency: Review, Approaches & Open Issues. Wireless Pers Commun 111, 1089–1115 (2020). https://doi.org/10.1007/s11277-019-06903-z

[8] B. D. Deebak, F. Al-Turjman, M. Aloqaily & O. Alfandi, "An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT," in IEEE Access, vol. 7, pp. 135632-135649, 2019, doi: 10.1109/ACCESS.2019.2941575.

[9] Zhang, Y., Deng, R. H., Han, G., & Zheng, D. (2018). Secure smart health along privacy-aware aggregate authentication & access control in Internet of Things. Journal of Network & Computer Applications. doi:10.1016/j.jnca.2018.09.005.

[10] Pawar R., Kalbande D.R. (2020) Elliptical Curve Cryptography Based Access Control Solution for IoT Based WSN. In: Raj J., Bashar A., Ramson S. (eds) Innovative Data Communication Technologies and Application. ICIDCA 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 46. Springer, Cham. https://doi.org/10.1007/978-3-030-38040-3_85

[11] S. Sawardekar and R. Pawar, "Data Security Approach in IoT Environment," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-7, doi: 10.1109/ICCCNT45670.2019.8944831.

[12] Han, J, Susilo, W, Mu, Y, et al. Improving privacy & security in decentralized ciphertext-policy attribute-based encryption. IEEE T Inf Foren Sec 2015; 10(3): 665–678.

[13] Ibrahim, M. H., Kumari, S., Das, A. K., Wazid, M., & Odelu, V. (2016). Secure anonymous mutual authentication for star two-tier wireless body area networks. Computer Methods & Programs in Biomedicine, 135, 37–50. doi:10.1016/j.cmpb.2016.07.022.

[14] Ullah, I., Alomari, A., Ul Amin, N., Khan, M. A., & Khattak, H. (2019). An Energy Efficient & Formally Secured Certificate-Based Encryption for Wireless Body Area Networks along the Internet of Things. Electronics, 8(10), 1171. doi:10.3390/electronics8101171.

[15] Li, F., & Hong, J. (2016). Efficient Certificateless Access Control for Wireless Body Area Networks. IEEE Sensors Journal, 16(13), 5389–5396. doi:10.1109/jsen.2016.2554625.

[16] Thakur, T. (2016). An Access Control Protocol for Wireless Sensor Network Using Double Trapdoor Chameleon Hash Function. Journal of Sensors, 2016, 1–6. doi:10.1155/2016/1210938.

[17] Kumar, P., Gurtov, A., Iinatti, J., Sain, M., & Ha, P. H. (2016). Access Control Protocol Along Node Privacy in Wireless Sensor Networks. IEEE Sensors Journal, 16(22), 8142–8150. doi:10.1109/jsen.2016.2610000.

[18] S. Bala, G. Sharma, & A. K. Verma, "PF-ID-2PAKA: pairing free identity-based two-party authenticated key agreement protocol for wireless sensor networks," Wireless Personal Communications, vol. 87, no. 3, pp. 995–1012, 2016.doi:10.1007/s11277-015-2626-5

[19] F. Li, Y. Han, & C. Jin, "Practical access control for sensor networks in the context of the Internet of Things," Computer Communications, vol. 89, no. 1, pp. 154–164, 2016.doi: doi.org/10.1016/j.comcom.2016.03.007

[20] Luo, M., Luo, Y., Wan, Y., & Wang, Z. (2018). Secure & Efficient Access Control Scheme for Wireless Sensor Networks in the Cross-Domain Context of the IoT. Security & Communication Networks, 2018, 1–10. doi:10.1155/2018/6140978.

[21] M. Li, H. Yuan, X. Yue, S. Muhaidat, C. Maple and M. Dianati, "Secrecy Outage Analysis for Alamouti Space–Time Block Coded Non-

RESEARCH ARTICLE

Orthogonal Multiple Access," in IEEE Communications Letters, vol. 24, no. 7, pp. 1405-1409, July 2020, doi: 10.1109/LCOMM.2020.2980825.
[22] Xiong, H.; Hou, Y.; Huang, X.; Zhao, Y.; Chen, C.M. Heterogeneous Signcryption Scheme from IBC to PKI With Equality Test for WBANs. IEEE Syst. J. 2021, 1–10
[23] Noor, F.; Kordy, T.A.; Alkhodre, A.B.; Benrhouma, O.; Nadeem, A.; Alzahrani, A. Securing Wireless Body Area Network with Efficient Secure Channel Free and Anonymous Certificateless Signcryption. Wirel. Commun. Mob. Comput. 2021, 2021, 5986469.
[24] Zhang, R.; Xue, R.; Liu, L. Security, and Privacy for Healthcare Blockchains. IEEE Trans. Serv. Comput. 2021.
[25] Chen, K.; Lu, X.; Chen, R.; Liu, J. Wireless wearable biosensor smart physiological monitoring system for risk avoidance and rescue. Math. Biosci. Eng. 2022, 19, 1496–1514.
[26] Amiet, D, Curiger, A & Zbinden, P 2018, 'FPGA-based Accelerator for Post-Quantum Signature Scheme SPHINCS-256', IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 1, pp. 18-39.
[27] Rashidi, B & Abedini, M 2018, 'Efficient Lightweight Hardware Structures of Point Multiplication on Binary Edwards Curves for Elliptic Curve Cryptosystems', Journal of Circuits, Systems, and Computers, vol.1, pp. 1-28.
[28] Gupta, U, Kalla, P & Rao, V 2018, 'Boolean Gröbner Basis Reductions on Finite Field Datapath Circuits using the Unate Cube Set Algebra', IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 38, no. 3, pp. 576-588.
[29] Singh, Laiphrakpam Dolendro, and KhumanthemManglem Singh. "Implementation of text encryption using elliptic curve cryptography." Procedia Computer Science 54 (2015): 73- 82.
[30] Nitha Thampi, Meenu Elizabath Jose,Montgomery Multiplier for Faster Cryptosystems,Procedia Technology,Volume 25,2016,Pages 392-398,ISSN 2212-0173,https://doi.org/10.1016/j.protcy.2016.08.123.
[31] Howe, J, Oder, T, Krausz, M & Güneysu, T 2018, 'Standard Lattice-Based Key Encapsulation on Embedded Devices', IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2018, no.3, pp. 372-393.
[32] Rabah, K 2017, 'Implementation of Secure-key Establishment and Generation using Elliptic Curve Cryptographic Protocols', Mara Research Journal of Computer Science & Security-ISSN 2518-8453, vol. 1(1), pp. 79-99.
[33] N. Saqib, F. Rodriguez-Henriquez, and A. Diazperez, "A parallel architecture for fast computation of elliptic curve scalar multiplication over GF(2m)", in Proc. of the 18th IEEE. International parallel and distributed processing symposium, 4004, pp.144
[34] S. Shohdy, A. Elsisi, and N. Ismail, "Hardware implementation of efficient modified Karatsuba multiplier used in elliptic curves", International Journal of Network Security, 2010, Vol.11, No.3, pp.138-145
[35] A. Rezai, and P. Keshavarzi, "High-performance modular exponentiation algorithm by using a new modified modular multiplication algorithm and common- multiplicand-multiplication method", in Proc .of the IEEE. World congress on internet security, 2011, pp.192-197.
[36] Samaila, Musa & Neto, Miguel & Fernandes, Diogo & M. Freire, Mário & Inácio, Pedro.(2018). Challenges of Securing Internet of Things Devices: A survey. Security and Privacy.10.1002/spy2.20. Url: wileyonlinelibrary.com/journal/spy2.
[37] Samanta, A., & Misra, S. (2018). Energy-Efficient and Distributed Network Management Cost Minimization in Opportunistic Wireless Body Area Networks. IEEE Transactions on Mobile Computing, 17(2), 376–389. doi:10.1109/tmc.2017.2708713.
[38] Elahe Fazeldehkordi, Iraj Sadegh Amiri, Oluwatobi Ayodeji Akanbi, Chapter 2 - Literature Review, Editor(s): Elahe Fazeldehkordi, Iraj Sadegh Amiri, Oluwatobi Ayodeji Akanbi,A Study of Black Hole Attack Solutions, Syngress, 2016, Pages 7-57, ISBN 9780128053676, https://doi.org/10.1016/B978-0-12-805367-6.00002-8.
[39] Priyambodo, T.K.; Wijayanto, D.; Gitakarma, M.S. Performance Optimization of MANET Networks through Routing Protocol Analysis. Computers 2021, 10, 2. https://doi.org/10.3390/ computers10010002.

Authors

Prof. Renuka Pawar is an Assistant professor in the Information Technology department at Sardar Patel Institute of Technology, Mumbai. Pursuing a Ph.D. from the computer department in the field of security in wireless sensor networks and having over 15+ Years of experience in teaching & research. Areas of interest include Linux operating systems, system and web security, network security, and WBAN security. Conducted various sessions on OWAPS, Ethical hacking, and digital forensics at various places. Published 15+ research papers in various conferences,2+ research papers in journals, and one poster in the research colloquium. Have participated and presented a research proposal in the final round of the 15th intercollegiate/institute/department Avishkar research convention 2020-21 organized by the university of Mumbai on July 1st, 2021.

Dr. Dhananjay Kalbande is a Professor in the Computer Engineering Department and Dean of Industry Relations at Sardar Patel Institute of Technology, Mumbai. With a Ph.D. in Technology from the University of Mumbai, a Post-Doctorate from TISS, Mumbai, and over 20+ Years of experience in teaching & research, my areas of interest include everything from Soft Computing (Neural Networks, Fuzzy Logic), Computer Networks, and more to Human Machine Interaction, Decision Making, Business Intelligence, Mobile Application Development and Technology for a social, healthcare development. In addition to authoring several books, have conducted several expert seminars on topics like NS2, Neural Networks, Machine Learning, Deep Learning, Python Programming, VB.Net, and ADO.Net. Published 115+ research papers in various conferences and 14+ papers in the journal. Have filled 3 patents and written 4+ books in the area of my expertise.

How to cite this article:

Renuka S. Pawar, Dhananjay R. Kalbande, "Privacy-Preserving Mechanism to Secure IoT-Enabled Smart Healthcare System in the Wireless Body Area Network", International Journal of Computer Networks and Applications (IJCNA), 9(6), PP: 746-760, 2022, DOI: 10.22247/ijcna/2022/217707.