CHAPTER 5

A HYBRID CIPHERTEXT-POLICY WITH HIERARCHICAL ATTRIBUTE-BASED RING SIGNCRYPTION TO ENHANCE SECURITY AND PRIVACY IN BODY AREA NETWORKS

5.1. INTRODUCTION

Wireless Body Area Networks (WBAN) has egresses as a central technology to offer real-time health monitoring and supervising. It helps patients by diagnosing many life-threatening diseases and getting the required medical attention from a remote location. To sense, sample, process and to communicate with physiological signals such as blood pressure, blood glucose level, blood oxygen saturation, heart rate, body temperature, blood pressure and physical activity such as level of activity, type and body posture along with environmental parameters such as atmospheric pressure, light, temperature, location, humidity multiple miniaturized network nodes has been designed.

WBAN operates in close vicinity to, on, or inside a human body and supports a variety of medical and non-medical applications. These miniaturized nodes can be placed in human body or in the users’ clothes as small patches. IEEE 802 has established a Task Group called IEEE 802.15.6 for the standardization of WBAN. The purpose of the group is to establish a communication standard optimized for low-power in-body/on-body nodes to serve a variety of medical and non-medical applications.

To monitor the daily activities BAN can be enabled to sense the physical activity, environmental conditions and health status. Data gathered based on the BAN nodes can be recorded, analyzed and merged in the personal server. The network coordinator of BAN plays the role of a personal server and can be executed either on smart phones or some dedicated devices. The data is given to the cloud, forwarded by the personal server hence it can be available for familiar caregivers, users’ investigation and approved health care providers. The healthcare application monitoring system can be integrated to provide assistance for living, oversee ambulatory therapy and individual monitoring of health to fitness. For instance, if the BAN is enabled by integrating with the smart phone applications, the monitoring of the individual daily activities can be recorded and the
feedbacks are forwarded to maintain optimal health. By the gathered information, the insufficient body mass index should be elevated based on the alert from the personal BAN server. Parameters such as height, age and gender values are recommended for monitoring.

The integration of personal server and BAN provides tele-medical system that comprises of medical personnel too. The medical server collects all the data related with the users and this can be extended over a period time. The preset markers available in the server indicate the significant changes occur in the human health status such as improvement or deterioration of the health status. The alert provided by the markers reminds the healthcare professionals to track the users. Added, the health status information provided by BAN used to monitor cardiac patients’ progress while rehabilitation in ambulatory settings, patients’ observance about treatment guidelines such as regular exercise, users effects on drug therapy and compliance.

5.1.1. POSSIBLE SECURITY THREATS IN WBAN

The WBAN applications targeted by the IEEE 802.15.6 standard are divided into medical and nonmedical applications as given in Fig. 5.1. Medical applications include collecting vital information of a patient continuously and forward it to a remote monitoring station for further analysis. This huge amount of data can be used to prevent the occurrence of myocardial infarction and treat various diseases such as gastrointestinal tract, cancer, asthma, and neurological disorder.

WBAN can also be used to help people with disabilities. For example, retina prosthesis chips can be implanted in the human eye to see at an adequate level. Non-medical applications include monitoring forgotten things, data file transfer, gaming, and social networking applications. In gaming, sensors in WBAN can collect coordinates movements of different parts of the body and subsequently make the movement of a character in the game, e.g., moving soccer player or capturing the intensity of a ball in table tennis. The use of WBAN in social networking allows people to exchange digital profile or business card only by shaking hands.
A WBAN is vulnerable to a considerable number of key attacks. These attacks are conducted in different ways, i.e., Denial of Service (DoS) attacks, privacy violation, and physical attacks. Due to restrictions on the power consumption of the sensor nodes, protection against these types of attacks is a challenging task. A powerful sensor can easily jam a sensor node and can prevent it from collecting patient’s data on regular basis.
5.1.2. WBAN ATTACKS

Like any other networks, WBANs are also vulnerable to various types of attacks. Attacks can be classified into four broad categories: snooping, modification, masquerading, and denial of service. In practice, an attack may employ several of these approaches. Based on the security requirements in WBANs, these attacks can be categorized as:

Attacks on secrecy and authentication:

It is where an adversary performs eavesdropping, packet replay attacks, or spoofing of packets. One example of eavesdrop attacks in WBANs is activity tracking of users. Based on the patient’s recorded data, it might be possible to analyze the activities of patients. This attack is very special to e-Health systems. (Kargl, F, et al., 2008) discussed a special kind of attack in WBANs. When a patient is being constantly monitored, it is possible for an attacker to analyze the amount of physical exercise he/she is performing by looking at heart rate and oxygen saturation data. Insurance companies might use this information to limit access to benefits for people with an unhealthy lifestyle.

Location tracking of users is another example of these attacks in WBANs. The attacker can eavesdrop the channel and capture the transmitted position signals in order to estimate the real-time patient location and even predict the patient’s likely destination. This attack hamper the patients location privacy because no one likes his/her location be tracked around the clock. One example of authentication attacks in WBANs is forging of alarms on medical data. In this case, attackers can simply create fake messages, which can lead to false system reactions e.g. to unnecessary rescue missions. The secrecy and authenticity of communication channels can be protected by standard cryptographic techniques and Message Authentication Code (MAC).

Stealthy attacks against service integrity

In this kind of attacks, the attacker attempts to make the network accept a false data value by changing the patient’s data before it reaches to the Personal Server (PS). For instance, an attacker can change a high blood pressure value to a normal blood pressure value. This is an undesirable and disastrous event. Integrity attacks can happen during times of transmission as well as storing. Message Authentication Code (MAC) techniques can protect WBANs from these attacks.
Attacks on Network Availability

These attacks are referred to as Denial-of-Service (DoS) attacks. DoS attacks attempt to make network resource unavailable to its users and affect the capacity and the performance of a network. Since WBANs are a kind of wireless sensor networks, they inherit most of DoS attacks from WSN, however, due to the unique characteristics of WBAN, there are some difference between DOS attacks that can take place in WBAN and WSN. In the following subsections, we explain DoS attacks in different layers of Open System Interconnection (OSI) model, from physical to transport layer. In addition, we discuss the applicability of these attacks in WBANs. DoS attacks on WBANs can be classified into four main categories as follows in Table 5.1.

Table 5.1. DOS ATTACKS ON WBANS

<table>
<thead>
<tr>
<th>Layers</th>
<th>DoS Attacks</th>
<th>Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Jamming</td>
<td>Spread-Spectrum, priority messages, lower duty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cycle, region mapping, mode change</td>
</tr>
<tr>
<td></td>
<td>Tampering</td>
<td>Tamper-proof, Hiding</td>
</tr>
<tr>
<td>Link</td>
<td>Collision</td>
<td>Error correcting code</td>
</tr>
<tr>
<td></td>
<td>Unfairness</td>
<td>Small frames</td>
</tr>
<tr>
<td></td>
<td>Exhaustion</td>
<td>Rate limitation</td>
</tr>
<tr>
<td>Network</td>
<td>Neglect and greed</td>
<td>Redundancy, probing</td>
</tr>
<tr>
<td></td>
<td>Homing</td>
<td>Encryption</td>
</tr>
<tr>
<td></td>
<td>Misdirection</td>
<td>Egress filtering, authorization monitoring</td>
</tr>
<tr>
<td></td>
<td>Black holes</td>
<td>Authorization, monitoring, redundancy</td>
</tr>
<tr>
<td>Transport</td>
<td>Flooding</td>
<td>Client puzzles</td>
</tr>
<tr>
<td></td>
<td>De-synchronization</td>
<td>Authentication</td>
</tr>
</tbody>
</table>
Physical Layer Attacks

Jamming Attack

Jamming is defined as interference with the radio frequencies of the body sensors. In this attack, the adversary tries to prevent, or interfere with the reception of signals at the nodes in the network. In doing so, the attacker sends a continuous random signal on the same frequency used by the body sensors. Affected nodes will not be able to receive messages from other nodes. In this attack, the adversary can use a few nodes to emit radio signals in order to disturb the transceivers’ operation and block the whole network. However, larger networks are harder to block in their entirety. The key point in successful jamming attacks is Signal to Noise Ratio (SNR), since WBANs usually suffer from vary low values of SNR, and also because these kinds of networks are small in size, the likelihood of successful jamming in WBANs is high.

Tampering Attack

In tampering attacks, sensors are physically tampered by an adversary. The adversary may damage a sensor, replace the entire node or a part of its hardware or even electronically interrogate a node to acquire patient’s information or shared cryptographic keys. Usually sensor devices have little external security features and hence prone to physical tampering. In a WBAN, the deployed sensors are under surveillance of the person carrying these devices, and therefore it is difficult for an attacker to physically access the nodes without this being detected. However, still there is a chance for tampering in WBANs. A good preventive measure against tampering is patient awareness. It could be very helpful to advice patients that only authorized people should be allowed to physically handle the devices (Al Ameen, M, et al., 2012).

Data Link Layer Attacks

Collision Attack

Collision attack is synonymous with the jamming attack that was just described. In this attack, the attacker listens to the channel, when he/she hears the start of a message, sends out its own signal that interferes with the message. This may cause a frame header corruption, a checksum mismatch, and therefore, the rejection of transmitted packets in
the receiver side. This attack is difficult to detect because the only evidence of a collision attack is the reception of incorrect messages. If a frame fails the Cyclic Redundancy Code (CRC) check, the packet is discarded. The countermeasures that can be applied to protect the WBANs from this attack are error correction mechanisms. The same as jamming attack, the likelihood of successful collision attack in WBANs is high.

**Unfairness Attack**

In unfairness attacks, network performance degrades because the medium access control layer priority is generally disrupted according to the application requirements. Use of small frames is a general defence against this attack.

**Exhaustion Attack**

Exhaustion of battery resources may occur when a self-sacrificing node always keeps the channel busy. In WSN, rate limitation is used to thwart this attack.

**Network Layer Attacks**

**Selective Forwarding**

Selective forwarding occurs when an adversary includes a compromised node in a routing path. When a malicious node receives a packet, it will do nothing and drop it. The malicious node can drop packets both selectively (just for a particular destination) and completely (all packets). Selective forwarding attacks are not applicable to the first communications level (intra-BAN level) of WBAN’s architecture, because in intra-BAN communications, the PS is usually in direct communication range of body sensors, hence body sensors can communicate with the PS directory, and they do not require to route packets. Body sensors which have very limited communication range select one nearby node to relay their information to the PS. In WBANs, routing is possible in the second level of communications (inter-BAN level), when multiple APs are deployed to help the body sensors transmit information. This way of interconnection extends the coverage area of a WBAN, and support patient mobility.

**Sinkhole Attack**

Sinkhole attack is similar to selective forwarding except that it is not a passive attack. In this attack, traffic is attracted towards the compromised or false node. This node
drops packets in order to stop packet forwarding. The applicability of this attack in WBANs is the same as selective forwarding attack.

**Sybil Attack**

In Sybil attacks, a malicious node - aka Sybil node, illegitimately claims multiple false identities by either fabricating new identities or impersonating existing ones. In WSNs, which involve routing, this attack can cause a routing algorithm to calculate two disjoint paths. In WBANs, at the intra-BAN level of communications, this attack can use feigned identities to send false information to the PS (Raazi, S. M. K. U. R., et al., 2010).

**Wormhole Attack**

Wormhole attack is carried out using two distant malicious nodes to create a wormhole in the target sensor network. Both malicious nodes have an out of band communication channel. One malicious node is placed near the sensor nodes when the other is placed near the base station. The malicious node, which placed near the sensor nodes, convinces sensors that it has the shortest path to the sink node through the other malicious node, which is placed near the sink node. This creates sinkholes and routing confusions in the target sensor network. Applicability of wormhole attacks in WBANs is the same as selective forwarding and sinkhole attack.

**Hello Flood Attack**

Many protocols require nodes to broadcast hello packets to announce themselves to their neighbours. When a node receives such hello packets, it may assume that the sender is in its neighbour. In case of hello flood attacks, this assumption may be false. An attacker with a high powered antenna can convince sensors that it is in their neighbour. In addition, the attacker can claim a high quality route and creates a wormhole. Although the creation of wormhole does not affect the intra-BAN communications of WBANs, Hello Flood attack in intra-BAN communications does cause body sensors to reply to the hello packets and therefore waste their energy.

**Spoofing Attack**

Spoofing attack targets the routing information exchanged between nodes (Karlof, C., et al., 2003), and attempts to spoof, alter, or replay the information with the intention to complicate the network. For example, an attacker could disturb the network
by creating routing loops, generating fake error messages and attracting or repelling network traffic from selected nodes. Applicability of spoofing attack in WBANs is the same as selective forwarding, sinkhole and wormhole attacks.

**Transport Layer Attacks**

**De-synchronization Attack**

De-synchronization attack targets the transport protocols that rely on sequence numbers. The attacker forges some messages with wrong sequence numbers and this leads to infinite retransmissions which waste both energy and bandwidth. WBANs are highly vulnerable against this attack. Since body sensors have a limited power budget, retransmissions could drain sensor’s power quickly and make them unavailable to the network. Authentication can be applied to thwart this attack.

**Flooding Attack**

Flooding attack is used to exhaust memory resources by sending a large number of connection setup requests. Since body sensors suffer from low memory space and therefore they are vulnerable against flooding attacks. In WBANs, The PS is very attractive target for flooding and also for other above mentioned attacks as it is heart of system. In WBANs, the PS is responsible to collects and analyzes all data sent by body sensors, and then transmits them to the remote health applications. If an attacker can make the PS unavailable to the network, he/she can block the whole system. In many cases, the PS is connected to the Internet which allows remote attacks, whereas attackers cannot have direct connectivity to the body sensors. It is essential to provide the PS with high power budget, enough memory space, and strong security mechanisms such as authentication, firewalls, and constant monitoring.

**5.1.3. CONSTRAINTS AND CHALLENGING PRACTICAL ISSUES**

To satisfy the above security and privacy requirements in WBANs, the research faced several challenging issues. These issues constrain the solution space and need to be considered when designing a security mechanism for WBANs. In the following subsections these major challenging issues and the constraints are discussed.
**Low Power Budget**

All sensors are constrained in terms of power budget, but the body sensors are more limited in this term. Energy is the crucial resource for body sensors since they use the power to perform all their functions like sensing, computation, and communication. Replacing this crucial resource in many scenarios is impossible or impractical especially for in-body sensors, which placed inside the human body. So energy limitation is one main consideration to develop WBAN mechanisms and protocols. The optimum energy consumption is a pivotal issue and algorithms that ensure minimum power consumption shall be preferred.

**Limited Memory**

Memory capacity in body sensors is very limited about few kilobytes. This limitation is because of small size of body sensors. However, the implementation of security mechanism may not need much memory, but keying material is stated in the sensor’s memory and takes up most part of the memory.

**Low Computation Capability**

Low computation ability in body sensors is caused by both low power budget and limited memory in body sensors. Since the main responsibility of body sensors is communication of the sensed information, therefore, there is very less amount of energy which can be expended on computation processes (Cherukuri, S, et al., 2003). Moreover, because of memory limitation in body sensors, they cannot perform heavy computation processes.

**Low Communication Rate**

Communication is the most energy consuming function in WBANs. In order to save energy, it is important to minimize the amount of communications in these networks. So, developers have to try to minimize the overhead transmissions required by other purposes rather than transforming of actual data.

**Environment Condition of WBANs**

Environment characteristics of WBANs pose additional security threads to these networks. Effective bandwidth of WBANs usually degrades due to effect of Radio Frequency (RF) emitting devices such as microwaves around the human body.
Furthermore, a number of studies prove that the human body presents different adverse fading effects to wireless communication channels that are dependent on body size and posture. In addition, to protect patients against harmful health effects associated with the RF emissions, the Specific Absorption Rate (SAR) in WBANs should be low. SAR is the rate at which the RF energy is absorbed by a body volume or mass. Because of SAR limitation in WBANs, body sensors must use very low power for transmission. This means that increasing transmission power beyond a certain level in order to reduce transmission losses in WBANs is impossible. Thus, in such environment, very low SNR values are expected.

However, interference and noise are generally QoS issues, but they have great potential to pose a serious security issues in WSNs and especially in WBANs. Since WBANs are naturally susceptible to channel fading and interference, and also they suffer from low values of SNR, even introducing a low level of noise into their channel can increase packet loss rates dramatically. Moreover, patient mobility increases the probability of packet loss in WBANs. It is clear that, in such environment, attackers can harm the system by simply presenting a low level of noise into the channel and causing a lot of packet loss.

In this scenario, lost packets should be retransmitted. Retransmissions cause the network to waste its bandwidth and sensors to exhaust their power supplies. Moreover, the system will suffer from long delays caused by retransmissions. Retransmission delays have a negative effect on data freshness, which is harmful especially for real-time applications. In some cases such as heart attacks, any delay in receiving the data could lead to fatality of the patients. Therefore, it is easy for attackers to harm WBAN by using the vulnerability of this network to the noise; they even can block the whole system by causing infinite retransmissions.

**Conflict between Security and Safety**

A strong access control mechanism should define existing users and regulations and firm guidelines regarding use of data for these users explicitly. Normally, e-Health care scenarios involve only a few and limited number of users such as doctors, nurses and supportive staffs. So, a strong access control for WBANs should not include other
specific users. However, it should be considered that too strict and inflexible data access control could prevent the timely treatment. In some cases, especially in emergency and disasters scenarios, disclosure of information to other people (such as mobile health teams) in order to serve the patients is necessary. So, a suitable access control mechanism in WBANs should be flexible enough to accept or compromise users to some extent.

**Conflict between Security and Usability**

As the operators of WBAN devices are usually novice, the devices should be simple and easy to use. Moreover, WBAN devices are supposed to be like the plug-and-play devices. Since the setup and control process of the data security mechanisms are patient-related, they shall involve few and intuitive human interactions. However, in case of WBANs security is more important than usability and omitting some manual steps to increase usability is not suggested.

**Lack of Standardization**

Each WBAN could include sensors from different manufacturers. Therefore, it is difficult to pre-share any cryptographic materials. In such networks that work with a wide range of devices, it is hard to implement security mechanisms that require the least common settings.

**5.1.4. ISSUES IN THE SECURITY STRUCTURE AND POSSIBLE SOLUTIONS**

IEEE 802.15.4 MAC has two operational modes: a beacon-enabled mode and a non-beacon enabled mode. In the beacon-enabled mode, the network is controlled by a coordinator, which regularly transmits beacons for device synchronization and association control. The channel is bounded by a super frame structure as illustrated in Figure 5.2. The super frame consists of both active and inactive periods. The active period contains three components: a beacon, a Contention Access Period (CAP), and a Contention Free Period (CFP). The coordinator interacts with nodes during the active period and sleeps during inactive period. There are a maximum of seven GTS slots in the CFP period to support time critical traffic. In the beacon enabled mode, a slotted CSMA/CA protocol is used in the CAP period. In the non-beacon enabled mode, the channel is accessed using unslotted CSMA/CA protocol.
Figure 5.2 IEEE 802.15.4 SUPER FRAME STRUCTURE IN A BEACON ENABLED MODE

Based on the study done on IEEE 802.15.4 security framework for WBANs by simulating smart, random, and weak attacks, the results showed that the smart attacker(s) has the capability of corrupting an increasing number of GTS slots compared to random and weak attackers. This means that the direct adaption of IEEE 802.15.4 security framework for WBANs is not reliable since most of the traffic in WBANs is carried in CFP period, which is most vulnerable to GTS attacks.

One of the solutions is to implement a sophisticated back-off detection scheme that should successfully detect the back-off attacks. However, the back-off detection scheme may not work for adversaries who have enough knowledge of the scheme. They may try to maximize their throughput and minimize their chances of detection. Another approach is to allow the receiver to assign the back-off window to the sender. In this scheme, the receiver can easily detect any attack and can even penalize the adversaries by increasing their back-off values. A game theoretic approach could also be useful to detect and prevent the attacks by considering that all nodes are selfish.

5.2. METHODOLOGY

In this research work, hybrid Cipher text-Policy Hierarchical Attribute-based Ring Signcryption (CP-HARS) is proposed for Body Area Network security. The initial process of proposed system is pre-processed the patient’s dataset using Enhanced Independent
Component Analysis (EICA). Then interoperability is defined by semantics and the semantic interoperability among body area sensor networks is used Ant Colony Optimization based Fuzzy Ontology (ACO-FO). The ACO-FO is used to improve the interoperability of BAN system. If the interpretability of communication failure occurs, it means BAN interaction does not progress as the external users. Once the problem has been identified and fixed, communication is then resumed using the updated ontologies. The proposed CP-HARS provides authentication, public verifiability, forwarding secret message confidentiality, veracity, non-refutation and message confidentiality. CP-HARS uses secure symmetric algorithm to encrypt messages quickly and provides security in establishing health monitoring and dealt with the resource constraint devices.

5.2.1. DATA PRE-PROCESSING USING ENHANCED INDEPENDENT COMPONENT ANALYSIS (EICA)

The dimensionality of the data is reduced using pre-processing in EICA. It is a method of presenting the patient’s data in a more comprehensible way by revealing the hidden structure in the data and often reducing the dimensionality of the representation. The BAN patient information contains more number of attributes. So EICA is used to reduce the attributes. A proper space has to be chosen, excluding the trailed Eigen values to improvise the generalization performance of ICA, in EICA. To get rid of the trailed Eigen value, ICA should precede space dimensionality reduction procedure before performing ICA whitening step. The generalization procedure of ICA can be enhanced and produce reduced computational complexity using the Principal Component Analysis (PCA) which belongs to a proper dimensionality reduction procedure.

Generalization analysis of ICA

ICA should precede space dimensionality reduction procedure before performing ICA whitening step, to get rid of trailed Eigen value. Excluding the trailed Eigen values to improvise the generalization performance of ICA is in EICA. To minimize the mutual information of the random vector, the independent component has three major steps: i) normalization, ii) rotations and iii) whitening. Initially, the random vector is transformed into unit covariance matrix in the whitening process. By higher order cumulants, the mutual
information is minimized by separating the source from independent components in the rotation operation. Lastly, in terms of phase (sign), norm and order a unique ICA representation is derived from the normalization procedure.

Specifically, let \( x \in \mathbb{R}^N \) be a random vector representing a patient attributes, where \( N \) is the dimensionality of the data space. The data present in the rows and columns, is concatenated to form a vector when the unit variables are not proportionate. The standard variable provides unit norms are so desirable. Standardization avoids using variable with large variance which dominates the other variables unduly.

Let \( \Sigma_x \in \mathbb{R}^{N \times N} \) be the covariance matrix of \( x \). The PCA of \( x \) defines an orthogonal eigenvector matrix \( \psi \in \mathbb{R}^{N \times N} \) and a diagonal eigenvalue matrix \( \Delta \in \mathbb{R}^{N \times N} \) with diagonal elements in decreasing order: \( \psi = [\psi_1, \psi_2, ..., \psi_N], \Delta = diag\{\delta_1, \delta_2, ..., \delta_N\}, \delta_1 \geq \delta_2 \geq \cdots \geq \delta_N \) be a projection matrix whose column vectors are the first \( n(n < N) \) leading eigenvectors of \( \Sigma_x \):

\[
P = [\psi_1, \psi_2, ..., \psi_N]
\]

The new random vector \( y \in \mathbb{R}^n \) in this reduced (\( n \)-dimensional) PCA space is defined as follows

\[
y = P^t x
\]

The ICA method implemented in this appropriately reduced (\( n \)-dimensional) PCA space is called as an Enhanced ICA method.

**Criteria for deriving EICA method**

The enhanced generalization performance of the EICA method depends on the appropriate PCA space where the EICA method is implemented. The two roles of the PCA procedure: for patient data attribute representation and for ICA generalization. From the representation point of view, to choose a PCA space that keeps as much information as possible in order to faithfully represent the original data. For example, the proposed methods consider attribute name of Blood Pressure (BP). It means that it can represent both the high BP and Low BP levels (range of values). The PCA space is used to separate this kind of information based data processing. Then the same space Eigen values are grouped under one clustering and other Eigen values are formed another cluster. The PCA space chooses by based on two criterions such as energy and magnitude criterion.
Energy Criterion

The transformation from the high dimensional space to a low dimensional one should be constrained in such a way that as much representative information of the original data is reserved as possible.

Magnitude Criterion

The reduced PCA space doesn’t include small-value trailed Eigen values, when implementing the EICA method.

Dimensionality of the reduced PCA space

Based on both the representation and magnitude criterion, ICA computation is resolute for reducing the dimensionality of the PCA. Representation criteria shows high dimensionality and magnitude criteria shows low dimensionality, the main goal is to attain the balance between the two roles of PCA procedure. Specifically, for enhanced generalization performance, EICA’s dimensionality reduction procedure should preserve a proper balance between the energy criterion—the need that the selected Eigen values account for most of the spectral energy of the original data, for representational adequacy, and the magnitude criterion—the requirement that the Eigen values of the covariance matrix in the reduced PCA space are not too small, for better generalization.

5.2.2. ANT COLONY OPTIMIZATION BASED FUZZY ONTOLOGY (ACO-FO) BASED APPROACH FOR IMPROVING SEMANTIC INTEROPERABILITY

The proposed system adopted the ACO based fuzzy rule ontology approach to support the semantic interoperability of the platform. The ACO used to improve the fuzzy rules. Ant Colony Optimization Algorithms for Learning Fuzzy Rule to apply ACO algorithms to a FRL problem, the following steps have to be performed:

Step 1: A FRL problem is obtained and it is represented as a graph or a similar structure easily covered by ants.

Step 2: Define the way of assigning a heuristic preference to each choice that the ant has to take in each step to generate the solution. Build the set of the input-output data pairs composed of the input-output data pairs that are located in the input subspace defined by

\[ E'_i = \{ e_i = (x^l_1, ..., x^l_n, y^l) \in E \text{ such that } \mu A_{il}(x^l_1) \ldots \mu A_{in}(x^l_n), \mu B_j(y^l) \neq 0 \}. \]
Step 3: Establish an appropriate way of initializing the pheromone. Pheromone value of each assignment is obtained as follows: $T_0 = \frac{\sum_{i=1}^{N_r} \max_{j=1}^{N_c} \eta_{ij}}{N_r}$.

Step 4: Define a fitness function to be optimized. The fitness function establishes the quality of a solution. The measure considered will be the function called mean square error (MSE), which defined as $MSE(RB_k) = \frac{1}{2|E|} \sum_{e_j \in E} \left( y^l - F_k(X_0^l) \right)^2$.

Step 5: Select an ACO algorithm and apply it to the FRL problem.

- The set of nodes attainable from $Ri$ (set of feasible neighbourhood of node $Ri$) will be $J_k(i) = \{ j \text{ such that } \eta_{ij} \neq 0 \}$ in the transition rules considered by both ACO algorithms when constructing the solution.

- The amount of pheromone ant $k$ puts on the couplings belonging to the solution constructed by it will be $1/MSE(RB_k)$, with $RB_k$ being the RB generated by ant $k$.

- In the local pheromone trail update rule of the ACO algorithm, the most usual way of calculating $\Delta T_{ij}, \Delta T_{ij} = T_0$, will be used, thus considering the simple-ACO algorithm.

- Then, from knowledge base, the system will retry all the ACO based fuzzy rules defined in the context. Fuzzy ontology calculates membership degree (ranging from 0 to 1) for each ontology class and applies a label with its degree. At this step, fuzzy ontology used for matching semantic strings from search patients details to fuzzy linguistic variables and terms.

5.2.3. CIPHER TEXT-POLICY HIERARCHICAL ATTRIBUTE-BASED RING SIGNCRYPTION (CP-HARS) FOR SECURITY

- In this subsection, the hierarchical attribute-based ring signcryption with cipher-policy is explained.

- If the hierarchy of the attribute is higher, then it is placed in upper level i.e. primary doctor and the attribute with lower hierarchy is placed in the lower level i.e. nurse is arranged in the matrix of HARS. This arrangement leads to hierarchical vectors or attributes, by sampling the attributes from the upper level
to lower level. Using delegation mechanism, new attributes can be added with the original attributes without the need of delegator, thus helps in knowing the secret key from the key generator.

- The proposed cipher text-policy HARS (CP-HARS), has been applied to the security information of BAN. In CP-HARS, the potential decryptors should consist of attribute vectors that generate an access policy in the cipher texts. Without considering attribute set and the subset, the higher level user can share the secret key with the user at the lower level. Later, the CP-HARS security can be defined. The public parameters, access policies, query of key with respect to set of attribute vectors and the created attribute vectors can be attained by the attackers in full security. The attackers project the challenge with the set of attributes and messages. In accordance with the challenge policies, two different messages are chosen for the generation of cipher text. To satisfy the access policy of challenge message, it cannot be distinguished which message has to generate cipher text and the attackers doesn’t provide query key associated with attribute vectors of set.

- By employing Linear Secret Sharing Scheme (LSSS), a CP-HARS scheme has been constructed to attain access structure of suitable expressiveness. An attempt has been made to construct CP-HARS from Hierarchical Identity-based Encryption (HIBE) by considering the attribute vector as an identity vector in the HIBE. The union of attribute vectors has to meet the access policy to meet the colluding users, when the straightforward construction is susceptible to collusion attacks, in which the coalition of users administers to decrypt cipher texts. Such attacks can be prevented in the future practice. By addressing the problem associated with randomization of secret keys to the users, with the help of well-determined dual encryption techniques, proves that the -HARS scheme is secure in the standardized model (i.e., without using random oracles) under the assumption of several non-instructiveness. The unimportant construction causes growth of public key size exponentially with the increased hierarchy size. While constructing, the public key is provided with maximum hierarchy size and it is linear and the cipher text size is sovereign of the user hierarchy or the number of users.
Linear Secret Sharing Schemes

A secret-sharing scheme $\pi$ over a set of parties $P$ is called linear (over $\mathbb{Z}_p$) if

1. The shares for each party form a vector over $\mathbb{Z}_p$.

2. There exists a matrix $A$ called the share-generating matrix for $\pi$, where $A$ has $l$ rows and $n$ columns. For all $i = 1, \ldots, l$ the $i$-th row of $A$ is labeled by a party $\rho_i$, where $\rho$ is a function from $1, \ldots, l$ to $P$. When consider the column vector $\mathbf{s} = (s, s_2, \ldots, s_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared, and $s_2, \ldots, s_n \in \mathbb{Z}_p$ are randomly chosen, then $A\mathbf{s}$ is the vector of $l$ shares of the secret $s$ according to $\pi$. If $A_i$ denotes the $i$-th row of $A$, then $\lambda_i = A_i\mathbf{s}$ is the share belonging to party $\rho_i$.

Notations and basic ideas

In a CP-HARS system, the attribute parameters are organized in a matrix, which consists of $L$ rows and $D$ columns and given by,

$$ U = (U_1, \ldots, U_l, \ldots, U_L)^T $$

Where $U_i$ is the $i$-th row of $U$ and contains $D$ attributes and $M^T$ denotes the transposition of a matrix $M$. We note that in each $U_i$ there may be some empty attributes which can be represented by a special symbol “$\phi$”.

The attribute vector of depth $k$ (or hierarchical attribute at level $k$) defined as

$$ \mathbf{u} = (u_1, u_2, \ldots, u_k) $$

Where for each $i$ from 1 to $k$, $u_i \in U_i$. This means that an attribute vector of depth $k$ is composed of $k$ attributes and the $i$-th attribute is selected from the $i$-th row of the attribute matrix. The $\mathbf{u}$ is a prefix of $\mathbf{u}$ if $\mathbf{u} = (\mathbf{u}, u'_{k+1}, u'_{k+2}, \ldots, u_k)$, where $k$ denotes the depth of $\mathbf{u}$.

Let $S = \{\mathbf{u}\}$ denote a set of attribute vectors and its cardinality is denoted by $|S|$. As stated in Definition 1, an access structure is a collection of non-empty subsets of a group of parties. Since the role of party is taken by attribute vectors, in a similar way define the access structure $A$ regarding attribute vector of depth $k$ such that $A$ is a collection of non-empty subsets of a set of all the attribute vectors of depth $k$. If a user possesses a set $S$ and $S \in A$, then $S$ is an authorized set in $A$ and we say this user or the set satisfy $A$. 125
The access structure of the multi-level LSSS is given in definition 2: depth of the attribute vector \( k \), access structure \( A \), with the product of \( i \)-throw the sharing matrix is generated. The \( i \)th matrix of the \( A \) in the injection function \( \rho \) maps with the depth of attribute vector \( K \), the hierarchical attribute is mapped with the row \( A \) in the injection function. The vector of the first coordinate is mapped with the depth of vector \( K \). In a CP-HABE system, a cipher text generated with an access structure \( A \) is decryptable by a key associated with set \( S \) under the condition that \( S \in A \). If a key for set \( S' \) is able to delegate a key for a set \( S \), it is required that each attribute vector of \( S \) have a prefix in \( S' \). This yields the concept of Set Derivation of two sets.

For a set \( S' \) of attribute vectors of depth \( k \) and a set \( S \) of attribute vectors of depth \( k + 1 \), we say that \( S \) is derived from \( S' \), denoted by \( S \leq S' \), if

\[
\forall \vec{u} \in S, \exists \vec{u} \in S', \text{ such that } \vec{u} = (\vec{u}, u_{k+1}) \text{ where } u_{k+1} \in U_{k+1}
\]

Modeling CP-HARS

The description of CP-HABE and its protection model is given. A CP-HABE system for message space \( M \) and access structure space \( AS \) consists of the following four (probabilistic) algorithms.

Setup (k)

The algorithm Setup takes no input other than the security parameter \( k \) and outputs the public key \( PK \) and a master secret key \( MSK \). Given a security parameter \( k \), the trusted Private Key Generator (PKG) first defines the set of universal attributes \( U \) in \( \mathbb{Z}_p \), where \( |U| = l \). After that, a \( d - 1 \) default attributes set from \( \mathbb{Z}_p \) is given as \( \Omega = \{\Omega_1, ..., \Omega_{d-1}\} \). Furthermore, PKG selects a pairing \( e: G1 \times G1 \to G2 \) where the order of \( G_1 \) and \( G_2 \) is prime \( p > 2^k \), and a generator \( g \) of \( G_1 \). PKG then chooses \( t_1, t_l, t_{l+1}, ..., t_{l+d-1} \in \mathbb{Z}_p \) randomly and computes \( T_i = g^{t_i} \text{ where } 1 \leq i \leq l + d - 1 \). PKG also picks \( \alpha \in \mathbb{Z}_p \) at random and computes \( Y = e(g, g)^\alpha \). Finally, PKG selects three cryptographic hash functions: \( H_1: G_2 \to \{0,1\}^{|M|} \times \mathbb{Z}_p^* \times G_1, H_2: \{0,1\}^* \to \mathbb{Z}_p^* \) and \( H_3: \{0,1\}^{|M|} \times \mathbb{Z}_p^* \to \mathbb{Z}_p^* \), where \( |M| \) denotes the length of the ciphertext. The public parameters \( PK \) are published as follows:
\[ PK = (G_1, G_2, e, g, \{ T_i \}_{i=1}^{l+d-1}, Y, H_1, H_2, H_3) \]

The master secret key \( MSK \) is denoted as \( MSK = (\alpha, \{ t_i \}_{i=1}^{l+d-1}) \).

**Key Extract (\( MSK, \omega \))**

To generate a secret key for the attribute set \( \omega \) of attribute vectors of depth \( \omega \subseteq u \), first choose random elements \( r \in Z_p, R_0, R_1 \in G_3 \) and compute

\[ K_0 = g^\alpha g^{aw} R_0, K_1 = g^w R_1 \]

Next, for each \( j \) from 1 to \(|S|\), pick random elements

\[ t_j \in Z_p, R_{(j,0)}, R_{(j,1)}, R_{(j,k+1)}, \ldots, R_{(j,l)} \in G_3 \]

For each attribute vector \( \vec{u} = (u_1, u_2, \ldots, u_k) \) of \( S \), choose \( v_x \) by finding \( u_1 \) as the \( x \)-th attribute of \( U_1 \) and compute its key component

\[
K_{(j,0)} = V_x^{\omega} \left( H_1^{u_1} \cdots H_k^{u_k} \right)^{t_j} R_{(j,0)}, K_{(j,1)} = g^{t_j} R_{(j,1)}, K_{(j,k+1)} = h_{k+1}^{t_j} R_{(j,k+1)}, \ldots, K_{(j,l)} = h_l^{t_j} R_{(j,l)}
\]

Outputs the private key \( D_S = (K_0, K_1, \{ K_{(j,0)}, \ldots, K_{(j,l)} \}_{j=1}^{|S|}) \).

**Signcryption (\( m, \omega_S, \omega_R \))**

To signcryption a message \( m \) to a receiver \( R \), the sender \( S \) follows the steps below:

- Chooses a subset \( \omega'_S \) with \( d \) elements from \( \Omega_S \) (where \( f \) attributes \( \{ i_1, \ldots, i_f \} \) are chosen from \( \omega_S \) to signcryption the message, and \( d - f \) attributes are chosen from default attributes set \( \Omega \)).
- The sender \( S \) randomly choose \( r \in Z_p^* \), and set \( s = H_3(m, r), U = g^s, \) and \( X = Y_s = e(g, g)^{\alpha s} \). Then computes \( E_i = T_i^S \) for each \( i \in \omega' \) and for each \( j \in \omega_R \).
- Let \( \omega'_S = \{ 1, \ldots, d \} \), and chooses \( k \in \omega'_S \) randomly. Defines the elements in set \( \omega'_S \cup \omega_R \) to be the ring. For \( l \in \omega'_S \cup \omega_R \) and \( l \neq k \), chooses \( U_l \in Z_p^* \) at random and computes \( h_l = H_2(m, U_l, X, \omega'_S \cup \omega_R, l) \), where \( |\omega'_S \cup \omega_R| = n_R + d \).
  For \( l = k \), chooses \( r_k \) from \( Z_p^* \) randomly and computes
Compute \( y = (m \| r \| V \oplus H_1(X)) \)

Finally, the ciphertext CT is denoted as \( CT = (y, \omega'_S, \omega_R, U, \{ U_l \}_{l=1}^{n_R + d}, \{ E_i \}_{i=1}^d, \{ E_i \}_{i=1}^n) \)

Unsigncryption CT

After receiving the ciphertext CT, R decrypts the ciphertext as follows.

- For \( CT = (y, \omega'_S, \omega_R, U, \{ U_l \}_{l=1}^{n_R + d}, \{ E_i \}_{i=1}^d, \{ E_i \}_{i=1}^n) \), select a subset \( \omega'_R \) with \( d \)-elements subset from attribute set \( \omega_R \).
- Computes
  
  \[
  X' = \prod_{j \in \omega_R} e(D_j, E_j)^{\Delta_j, s(0)} \prod_{j \in \omega_R} e\left( g, g^{t_j} \right)^{\Delta_j, s(0)}
  \]

  And retrieves \( m', r', V' \) as \( (m' \| r' \| V') = y \oplus H_1(X') \)

- Computes \( s' = H_3(m', r') \) and verifies whether \( U = g^{s'} \) holds or not.

- For \( l \in \{1, ..., n_R + d\} \), computes \( h'_l = H_2(m, U_l, X, \omega'_S \cup \omega_R, l) \) and verifies \( e(g, \prod_{l=1}^{n_R + d} U_l, g^{t_l, h'_l, s'}) = e(g, V') \) holds or not. If so, R accepts CT as the valid ring signcryption on the message \( m' \); R rejects otherwise.

The depth of the system is small in its maximum practice. The system public key is linear, when the number of attributes in the matrix is linear with the number of total attributes in the system. With the deepest level, the attribute vector is linear with the size
of the secret key along with the linear depth of the number of available attribute vectors. At the setup phase, the pair is pre-computed hence no signcryption algorithm is needed in pairing operation. The cipher texts are independent at the receiver side; in the receiver hierarchy and access structure with the number of attribute vectors are also linear. When the access structure of the attribute vector is linear, the pairing operation also satisfies the decryption algorithm.

5.3. EXPERIMENTAL RESULTS

In this section, the performance of proposed system is evaluated and the results are compared with the existing methods of ARSS and ECC with FO signcryption (Arul Jothi, A, et al., 2016). A quantitative performance analysis is presented in this section. The energy consumption during message transmission and computation time are the principle areas of concern of this section. The size of the message being transmitted is analyzed, in which the energy consumption related directly with the message size.

Message Size

The size of the complete cipher text is computed in this scheme. The cipher text is the concatenation of time, message and attributes. Figure 5.3 illustrates the affiliation between the number of users and the total message size at various levels of security. The message size with respect to the number of users is indicated by curves in the Figure 5.3.
Figure 5.3 MESSAGE SIZE VS. NUMBER OF USERS

Figure 5.4 shows the functional relationship between the message size and the security level and the message size has a linear relationship with the security level is observed. It also shows the proposed CP-HARS achieved high level of security as compared to the existing ARSS and ECC with FO signcryption schemes.
Communication Overhead

From the point concerning with communication, signcryption plays a vital role in contributing communication overhead. The overhead associated with the signcryption is the size of the message. The overhead for signcryption and designcryption are $5|q| + 4$ and 1 respectively. The relationship between the security level and communication overhead is represented in Figure 5.5. The communication overhead for the proposed CP-HARS increased along with the increase in the security level.
The energy consumption of Signcryption in CP-HARS is calculated from the formula $E = U \times I \times T$, where $I$ is set of individual objects, $T$ is code running time. However, while the public and private key generation speeds have been increased, encrypting and decrypting large volume of data is slow in existing system. The energy cost of fuzzy, Sign-then-Encryption, ECC with FO and ARSS are compared to CP-HARS signcryption energy consumption to show that CP-HARS significantly reduces energy consumption. The results provide a very compelling argument for ARSS, showing that, based on an assumed battery life, the device using ARSS could execute the number of key exchange operations.

Figure 5.5 illustrates the relationship between the Energy consumption on communications and the number of users. CP-HARS has a less power computation than other schemes. Energy consumption while performing communication and computation...
is considered inclusively. When the number of users is higher, CP-HARS performs efficient communication. The energy consumption of CP-HARS is lesser when compared to the ECC with FO signcryption and ARSS scheme.

![Figure 5.6 ENERGY CONSUMPTION ON COMMUNICATIONS WITH RESPECT TO THE NUMBER OF USERS](image)

**Figure 5.6 ENERGY CONSUMPTION ON COMMUNICATIONS WITH RESPECT TO THE NUMBER OF USERS**

**Computational Cost**

The cost of a computation as the message of the time taken by the computation and the cost of the hardware used for the computation. Figure 5.7 demonstrates the computational cost of CP-HARS signcryption with other schemes. The observation can figure out as follows: initially, the computational cost of signcryption is lesser compared to the other schemes. Energy consumption while performing communication and computation is considered in cursively. When the number of users is higher, CP-HARS performs efficient communication. Signcryption shows rapid development since it is an emerging technique. CP-HARS provides better secured communication, since BAN controller provides less computation capacity between the external devices and controller. CP-HARS is achieved less computation cost compare than existing ARSS and ECC with FO signcryption schemes.
5.4. SUMMARY

A Body Area Network (BAN) is a wireless network of health monitoring sensors designed to deliver personalized healthcare. Securing inter-sensor communications within BANs is essential for preserving not only the privacy of health data, but also for ensuring safety of healthcare delivery. The proposed CPHARS is compared to existing Attribute-based Ring Signcryption Scheme (ARSS) and Elliptic Curve Cryptography with Fuzzy Ontology (ECC with FO) signcryption. In this research, the proposed cryptosystem was subjected to as Cipher text-Policy Hierarchical Attribute-based Ring Signcryption (CPHARS) proposed for BAN security to ensure its versatility. The initial process of proposed system is pre-processed the patient’s dataset using Enhanced Independent Component Analysis (EICA). Then ACO-FO is used to improve the interoperability of BAN system. A CP-HARS scheme is constructed with short cipher texts. The scheme is proven to be secure in the standard model under non-interactive assumptions. The experimental output provided unforgeability, authenticity, non-repudiation and confidentiality to achieve higher security, lower energy consumption, lesser computational cost and communication overhead.