A Hybrid Cryptography and Authentication based Security Model for Clustered WBAN

1 Aarti Sangwan, 2 Partha Pratim Bhattacharya

1,2 Mody University of Science and Technology, Laxmangarh, Rajasthan, India - 332311

Email: 1 aarti.sangwan1@gmail.com, 2 hereispartha@gmail.com

*Corresponding author: Aarti Sangwan

Abstract

The communication in a clustered WBAN is performed at different levels through multiple nodes and controllers. This kind of multi-level involvement of nodes opens the nodes for security leaks. In this paper, a dual level security is integrated using hybrid cryptography method. A hybrid authentication and cryptography based method is defined for identity and information level security. The hybridization of security for clustered WBAN is achieved using RSA and hash key encoder. The RSA is here applied for node to controller for identification and verification whereas SHA is applied for reliable symmetric message encoding for node-to-controller and controller-to-controller communication. The proposed security model is applied in an integrated form to the clustered WBAN network to improve communication reliability. The proposed secure communication model has improved the performance of the network. The simulation is applied on clustered WBANs with different number of WBANs. The comparative simulation results show that the proposed model has effectively improved the packet communication and network life.

Keywords: Body Area Network, Clustered, Secure, RSA, Hashcode

I. Introduction

In a single WBAN [XXVI] [XII] network the sensor devices are placed on or in human body to monitor the specific organ or the disease. The information captured through these sensor devices helps to diagnose the disease instantly and immediate treatment can be supplied. These sensor devices are also connected to a
centralized portable device or the coordinator. This coordinator connects and transfers this collected information to physician, hospital or health organization to inform about health status of the person. This kind of connected communication can be done through WLAN or GPRS or through internet connection. The WBAN architecture and its communication with global environment is shown in Figure 1. The communication architecture of EHealth communication is divided into three tiers. In first tier, the WBAN network captures the communication through body sensors. In second tier, the information is filtered and managed at WBAN controller. In third tier, the summarized and effective information is transformed to centralized database through web.

The more critical network scenarios exist, when number of WBAN networks exists in the same geographical region such as patients in a hospital or athletes in a sports campus etc. In such scenarios, the multiple WBANs are monitored collectively respective to common communication schedule.

Figure 1: WBAN Communication Architecture

This kind of parallel communication can increase the network load on available resources and it can result in the degradation in network performance and reliability in network communication. Various network architectures are defined by the researchers to reduce the parallel communication and to improve the communication reliability in the network. The clustered [XX][III] communication is one such architecture in which network is divided in smaller geographical
segments. Each generated cluster is controlled by the dynamically generated cluster head. The nodes within the cluster head communicates to its cluster head and the cluster head collects this information and delivers it to base station. The cluster communication provides the effective and reliable data delivery in a distributed WBAN network. But as the network size increases and the communications are open at different levels, the security challenges also increase in the network. The network can be infected from different kinds of internal and external attacks to capture the network information and to disturb the communication flow. The sensitive information of patients can be leaked through these network attacks.

In a WBAN network, sensitive personal information of patients is transmitted at different levels. This network requires security in terms of confidentiality, integrity and authenticity. In WBAN, different levels of security exist and demanded by the individuals. At the lowest level of security, the communication is performed without any individual verification and without setting up any confidentiality protection. At first level, the authentication level security is applied. At this level, communication is performed only to and through the verified nodes. The information of authenticated users is maintained in the base station in a distributed network. In case of clustered network, the information of authenticated users is maintained on cluster controller. Various password specific and key specific authentications can be performed on clustered network. At the highest security level, the encrypted communication is performed through verified nodes. The authentication and cryptography is applied in combined form. Various symmetric and asymmetric cryptography methods are available to provide secure communication in WBAN network. Each cryptography method defined by work stages includes key generation, key distribution, data encryption and data decryption. In a distributed and clustered network, key management has the greater significance to achieve the effective and secure communication. The generated keys can be same or different for encryption and decryption process. Based on this, the cryptography method can be symmetric or asymmetric. Once the key is generated, the distribution of keys is done either by the controller, source or third party. The secure sharing of these keys is also a challenge in distributed network. A set of generated keys can be applied for a particular session of communication. These session specific keys are generated dynamically in next session for initiation of communication.

In this paper, dual level security model is integrated to a clustered WBAN. The user identity and secure data communication based security aspects are included while performing the different levels of communication in clustered network. RSA based authentication and symmetric hash encoding is applied for secure node-to-controller and controller-to-controller communication. In this section, the description of WBAN architecture and distributed WBAN architecture is provided. The security challenges faced in distributed and clustered WBAN network are also
defined in this section. In section II, the work provided by earlier researchers for WBAN and secured WBAN communication is discussed. In section III, the proposed dual security model integrated with clustered WBAN network is discussed. The algorithm for secure communication in clustered WBAN is also provided in this section. In section IV, the comparative results obtained for proposed security model are presented for different size networks. In section V, the conclusion of work is presented.

II. Related Work

Like other networks, security is critical challenge in distributed and clustered WBAN. Security flaws not only leak the valuable information but also degrade the network life and performance. The network and node level securities, methods were defined by the researchers to prevent and detect these security attacks and leaks. Authentication and cryptography methods are most considered phenomenon to secure the distributed WBAN. Kompara et al [XI] has provided a detailed study on various security challenges and relative security methods. Various key agreement schemes and their strengths and limitations are discussed by the researcher. Another study on key management and cryptography methods was provided by Masdari et al. [XIX]. The capabilities of biometric and non-biometric methods were explored by the author. Various security protocols invested by the researchers were discussed by the author. Ali et al. [I] has divided the available key agreement based secure communication in three main categories called Physiological value based schemes, non-physiological value based schemes and hybrid schemes. The characterization of these schemes using adequate metrics was provided by the author. Al-Janabi et al. [III] has identified the challenges in WBAN network for health care system. The security requirements, threats, protocols and models were discussed by the author. In this section, various security and reliability enhancement methods suggested by the earlier researchers are discussed. The physiological [IV] feature based hybrid key management scheme was provided. The feature and data selective encryption method was defined by the author.

In single WBAN where the sensitive medical information is maintained in centralized controller, secure communication is required by the medical authorities. The protocols and routing methods can be integrated with encoded and authenticated communication to improve the network reliability. One such integration of security aspect to AODV protocol was provided by Raja et al. [XXIII]. Author applied the security using RSA encrypted nonce. The message level security integration improved the reliability of complete network. An anonymous [IX] authentication scheme was suggested to secure the identities of patients. In this scheme, no information is maintained for node verification. The location and communication feature based observations were applied to improve
the network security. Li et al. [XVII] has correlated the RSSI values as authentication coefficient. The inter-node distance and noise vectors were used to estimate the RSSI values and to allow secure communication over the network. A lightweight [V] cryptography method was introduced for three-tier communication architecture in WBAN. The method had low memory and energy requirements. Prameela et al. [XXII] has applied hash chain to improve the security in WBAN. The protocol was defined with instant authentication and complement to control node compromise. The restricted node based authentication and encoding method improved the reliability of the WBAN network. A Zero Knowledge Proof (ZKP) [X] based identity verification method was suggested to verify the node commitment. The method was effective against message based replay and injection attacks. The method was defined with low resources and memory requirements. A key reconstruction [VIII] based protocol was suggested as gateway to WBAN network to achieve secure long-term communication. This backup gateway was established to achieve the reliable communication in healthcare systems. The session token based recovery method provided the reconnection without revealing the identity of the node. Salehi et al. [XXIV] has proposed a practical authentication scheme to achieve effective privacy along with the avoidance of information reconciliation. In this method, the smaller secret keys were generated for short frames for enabling the symmetric encoded communication in body adhoc networks. A key agreement based hybrid [VII] authentication method was provided in which identity driven cryptography was applied between the smartphone and storage site and symmetric cryptography was achieved between the nodes and the smart phone. This dual phase cryptography method improved the reliability of WBAN communication.

Li et al. [XVIII] has proposed a group based cooperative group solution to improve the security and reliability. In this method, the RSSI information is used for key generation with multi-fold density and data similarity analysis. The group adaptive key sharing and communication improved the communication aspects without any security threat. An improvement on Reed-Solomon encoding was provided by Li et al. [XVI] to improve the performance of secure communication. The effective key agreement was developed between the sensor and controller to achieve efficiency and security. A multi-layer authentication [XXV] protocol was suggested with session key specific secure communication in WBAN. Author defined secure one-to-many group communication by generating the group keys with low computational cost. The ECC (Elliptic curve cryptography) was integrated to generate the session keys and cryptography between node and controller. Wei et al. [XXVII] has proposed the anonymous authentication scheme based on low-entropy communication on a random oracle model. The password specific authentication and cryptography method provides easy access of the system to an authenticated person. The low-entropy based password improved the security with low complexity contribution. A lightweight anonymous
authentication [XIII] based key agreement scheme was suggested for reliable two-hop communication in WBAN. The unlinkable and anonymous session key was generated to validate the formal proof for WBAN architecture. A three-factor [VI] user authentication and key agreement based secure communication was provided in WBAN system. The functional and dynamic features and updates were used to improve the security of the network. Li et al. [XV] has proposed an improvement to 1-round authentication protocol using user anonymity. Liu et al. [XIV] had proposed two key exchange protocols based on symmetric cryptosystem to achieve selective authentication. Two pair of session keys was generated under node certification to gain high level security with light computation.

In clustered WBAN and sensor networks, the communication is performed at different levels between nodes and controllers. Researchers have applied various symmetric and asymmetric cryptography methods for effective shared communication in the network. Mehmood et al. [XX] has defined a two phase security method applied on inter-cluster communication using multiple key distribution schemes. The inter-cluster based key agreement method was suggested to prevent the network from the intrusion attacks. A hybrid [II] security framework for inter-WBAN and intra-WBAN was provided for pairwise key agreement. The physiological value based key generation and refreshment was integrated to LEACH protocol to enable secure clustered communication. An asymmetric block [XXI] encryption scheme was integrated to improve communication privacy and security in clustered WBAN. The elliptic key was used to generate public-private key pair and to provide secure communication between nodes. The light weight keys improved the security strength at different level of communication in the network.

III. Materials and Methods

The WBAN networks presented in a limited area perform the parallel communication to a base station for distribution of collected sensitive information. The information carried over the open network is personal information including patient identity, health status, disease characterization etc. This information is captured from numerous patients in same schedule and required to transmit to centralized data centre. This kind of scheduled information transition increases the load in terms of parallel communication. Another issue while communicating such sensitive information in open network is the security threat. The distributed WBAN network can be infected from various internal and external attacks. In this paper, an effective communication architecture for WBAN is provided to resolve all the defined issues. In this proposed solution, to resolve the problem of network load and parallel communication, the network is transformed to clustered architecture. The clustering is the core phenomenon applied in this work to achieve segmented communication separately for different geographical regions.
In this architecture, the network is divided in smaller regions and the information of each region is collected by the region controller. These controllers finally deliver the sensitive information to base station. In this way, the restricted features of distributed WBAN networks are utilized effectively by clustered architecture and the reliable communication is performed. After setting up the clustered architecture, the security shield is applied to the network to verify the node identity and to provide secure communication. A hybrid security model is implied in clustered architecture to gain high level of security. The security effective clustered architecture for WBAN network is shown in Figure 2. The architecture enables the identity level security at controller level using RSA approach and provides the encoded communication using hashcodes. This secure and reliable communication model has improved the reliability and performance of clustered WBAN.

Figure 2: Proposed Hybrid Secure Clustered WBAN Architecture

III.a Generation of Distributed WBAN

The proposed security architecture is defined to enable the secure and reliable communication in distributed clustered WBAN architecture. The network is generated in restricted geographical region such as hospitals or the sports club. Various patients or athletes with wearable sensor devices can be observed in parallel within the coverage region. These individuals are represented as the smaller WBAN network in itself. Each of WBAN network defined is defined with 9 body sensors to monitor different organs. These organs can be heart, brain, blood pressure and body moments. These WBAN networks are distributed over the restricted region at random locations. The features of this distributed network are shown in Table 1.
Table 1: Features of Distributed WBAN

<table>
<thead>
<tr>
<th>Features</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>WBAN Size</td>
<td>9 Body Sensors</td>
</tr>
<tr>
<td>WBAN Node Energy</td>
<td>Sum of energy of all body sensors</td>
</tr>
<tr>
<td>Geographical Region</td>
<td>100x100 Meter</td>
</tr>
<tr>
<td>Number of WBANs</td>
<td>100 Nodes</td>
</tr>
<tr>
<td>Topology</td>
<td>Random</td>
</tr>
<tr>
<td>Controller</td>
<td>Fix with All authorization</td>
</tr>
<tr>
<td>Coverage</td>
<td>30 Meter</td>
</tr>
</tbody>
</table>

Table 1 shows all the construction level configurations of WBAN network. The configuration with relative features is shown in the above table. In this network, 100 WBANs are placed at random position with communication characterization of individual WBAN. After setting up the network, the communication and security features are applied for secure and reliable communication.

### III.b Formation of Balanced Clustered Architecture

The distributed WBAN network is transformed to secure clustered architecture. Before integrating the security aspects in WBAN network, the transformation of this distributed network is done to clustered form. In this research work, a balanced and energy effective clustered architecture is generated to utilize the available limited resources efficiently. As discussed in previous subsection, the WBAN nodes are defined with limited energy and sensing range. To avoid the parallel and short distance communication, the network is divided in smaller segments called clusters.

In this paper, energy, cluster load and region load effective method is defined for cluster generation and communication. Each of the clusters is having a centralized controller to collect the health information of patients. The node to controller communication is performed through multihop path. Once the patient data is collected on the controller, the aggregative clustered data is transformed to base station. For this communication, the multihop controller-to-controller communication is performed. The process of controller identification and communication is shown in Table 2.

The algorithmic process of cluster generation and initiation of the communication is shown in Table 2. The clustering process works on the distributed WBANs. Each of the WBAN is processed under energy and round adaptive probability vector to identify the expected controller nodes. For each of these expected
controllers, the coverage nodes are identified. This coverage density is analysed in terms of number of member nodes and number of controllers in the network.

Table 2: Generation of Balanced Clustered Architecture

<table>
<thead>
<tr>
<th>ClusteredCommunication(WBANs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/<em>WBANs is the list of WBAN nodes distributed in restricted network</em>/</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>1. For i=1 to WBANs.Length</td>
</tr>
<tr>
<td>//Process the network*/</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>2. If (WBANs(i).E &gt; ETthreshold And WBANs(i).Prob&gt;Threshold)</td>
</tr>
<tr>
<td>//A node with high energy and high probability is considered for effective selection of cluster controller*/</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>3. If(Load(WBANs(i))&lt;LThreshold And RegionLoad(WBANs(i))&lt;RThreshold)</td>
</tr>
<tr>
<td>/<em>Check for the capability of node for load balanced network formation</em>/</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>4. Set Controllers.Add(WBANs(i)) /<em>Set Node As Controller</em>/</td>
</tr>
<tr>
<td>5. Members=GetMembers(WBANs(i),Coverage) /<em>Get Cluster Members</em>/</td>
</tr>
<tr>
<td>6. PerformCommunication(WBANs(i),Members) /<em>Perform Cluster adaptive communication</em>/</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
</tbody>
</table>

Both these parameters are analysed under load limit to decide the node as controller. After considering two level load vector, a balanced and load effective cluster is generated and cluster controller is identified. Each of the controllers is analysed under the sensing range to identify the cluster members. Now the communication is initiated between the node to controller and controller-to-controller for effective data delivery to the base station.

III.c Secure Clustered Architecture

Two phase security is applied on the generated clustered WBAN network to achieve secure and reliable communication. These two phases cover both the aspects of high level security. In first phase, the WBAN node verification is done using public key cryptography method. In this stage, RSA is applied for authentication of WBAN for specific cluster head. The controller node maintains the information of these authenticated WBANs. The key generation, distribution and management is also done at the controller node. The RSA is the public key cryptography method which generates two keys called public key and private key.
As the communication session begins, the controller node generates the public-private key pair for cluster member. The private key is stored in the controller itself and the public key is assigned to the WBAN node. As the communication begins, the node level authentication is performed by generating an encoded information block to controller node. The controller node, accept this encoded information block and perform the decryption using private key of that node. The RSA based encryption and decryption of data block is performed to authenticate the node on particular controller. If the node is not authenticated, the communication failure occurs. The authenticated node based communication is considered as the valid authenticated communication. At second level of security, the encoded communication is performed using SHA algorithm. At the WBAN controller, the health information of patient is divided in smaller blocks and data encoding is done using SHA algorithm. The SHA encoded data is finally received at the centralize data center exist here in the form of base station. The data decoding is done at the receiver end by performing the reverse mathematical operations on each encoded block. These individually retrieved message blocks are finally combined to build the complete message. The algorithmic approach used by the RSA and SHA encoders is described in sub sections of this section.

A) RSA

RSA (Ron Rivest, Admi Shamir and Leonard Adleman) is the public cryptography algorithm used as digital signature. It is able to verify the authenticity of an individual. In this research work, RSA algorithm is applied to authenticate a WBAN within the coverage of a controller. The algorithm for cryptography method or digital signature specific authentication is provided in Table 3. In this method, a public-private key pair is generated. The public key is distributed to the nodes to perform the data encryption and the private key is maintained by the receiver node. Each public key user can encrypt the data packets but decryption cannot be performed. The receiver node is having the private key and by using this key, the data can be retrieved back from encoded packet.
Table 3: RSA Based Key Pair Generation

<table>
<thead>
<tr>
<th>RSA(p,q)</th>
<th>/<em>p and q are the randomly generated prime numbers used for key pair generation</em>/</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Set n=p*q /<em>Generate part of public key</em>/</td>
</tr>
<tr>
<td>2.</td>
<td>Set delta = (p-1) (q-1)</td>
</tr>
<tr>
<td>3.</td>
<td>Generate e such that 1 &lt; e &lt; delta /<em>generate public key exponent</em>/</td>
</tr>
<tr>
<td>4.</td>
<td>Compute d, where d* e ≡ 1 mod delta /<em>Generate private key exponent</em>/</td>
</tr>
<tr>
<td>5.</td>
<td>Return (n,e) and (n,d) as public and private key pairs</td>
</tr>
</tbody>
</table>

Table 3 has shown the algorithmic process for key pair generation for RSA based node authentication. Once the key pair is generated, the message block can be encoded using (n,e) key pair on WBAN node. The encryption equation is shown in equation (1)

$$\text{CipherMsg} = \text{Msg}^e \mod n$$

Where (n,e) is the public key pair

Msg is the plain message block

CipherMsg is the generated encoded message

The generated encoded message is transmitted by the WBAN node to the cluster controller. The cluster controller accepts this message and performs the data decoding. The decryption equation using private key of that particular WBAN is shown in equation (2)

$$\text{Msg} = \text{CipherMsg}^d \mod n$$

Where, (n,d) is the private key pair

CipherMsg is the encoded message block

Msg is the retrieved message block

B) SHA

SHA (Secure Hash Algorithm) is the cryptographic hash function designed to encode the message. The algorithm is defined under the digital signature standard to generate the block ciphers. Algorithm for hash code generation is shown in Table 4. SHA includes a series of mathematical and logical operations applied on each message block to generate the encoded data. The regulation of encoding is done through specification of mathematical function and constants.
Table 4: SHA Based Message Encoding Algorithm

```
SHA(Msg)
/*Msg is the plain message processed under hash code to generate the encrypted message*/
{
1. Msg=Padding(Msg) /*Add the padding to bit message to transform the message in multiple of 64 bits*/
2. Msg = Append(Msg, 64Bits) /*Append the 64 bits to the padded message*/
3. Func=GeneratePFunction() /*Generate the mathematical and logical processing function to perform message encoding*/
4. Cost=PrepareCostants() /*Generate the processing constants to perform message encoding*/
5. Space=InitializeBuffer() /*Allocate the space for block specific message encoding*/
6. Encoded=ProcessMessage(Msg,Func,Cost) /*Apply the functions on message blocks for generation of encoded data*/
7. Return Encoded
}
```

These identity effective and cryptography based methods are integrated to the clustered communication to achieve the secure communication in the network. The simulation environment and the relative results obtained for different networks are provided in next section.

III. Results and Discussions

The proposed hybrid security model is defined to improve the reliability and performance of clustered WBAN. The model is defined to ensure the authenticated and encoded communication. The architecture is defined under multiple-parameters based analysis defined at multiple levels to achieve load and energy sensitive clustering. The security is here applied at node-to-controller level communication and controller-to-controller communication. RSA is here considered as the asymmetric cryptography method for node identity verification and hashing is used to achieve the secure symmetric communication over the network. The simulation of this model is done in randomly clustered WBAN network. The network is generated initially with random energy, position parameters and with specification of node and network level constraints. As a node participates in the network, the node verification is done using RSA method and encoded communication is performed. Each node involved in the communication gives some amount of energy loss being transmitter, receiver and forwarder node.
The communication is performed for 2000 number of rounds and the observations are taken for different instances of time. The comparative results are taken against the RSA based WBAN network. In the existing approach, the cluster switching is performed more frequently because of which the authentication is performed again and again whereas the proposed method provided the stable cluster formation and it improved the network performance and reliability. For more robust analytical decision, the simulation is applied on networks with 10, 20, 50 and 100 WBANs. The comparative results are generated in terms of dead node count, packet communication and remaining energy parameters for different number of rounds and for different size networks.

The reliability of a network can be identified based on the number of nodes performing the communication. Initially, the network is defined with 100 alive nodes, but as the communication is performed, the nodes start losing their lives. A network is more reliable if less number of nodes are dead. Figure 3 is showing the comparative analysis in terms of dead node existence in the network. Here, x axis shows the number of communication rounds and y axis shows the dead nodes occurred during these communication rounds. The brown bars shows that the dead
nodes in existing approach are lesser than existing secure clustered WBAN. The results show that the proposed hybrid security model has improved the reliability of the network.

The main objective of network architecture is to perform the reliable communication and to improve the communication rate. In clustered network, the intermediate attacker node or load can result in communication failures. Figure 4 shows the comparative results of proposed hybrid security model in terms of network communication. Here X axis shows the number of communication rounds and y axis shows the packets successfully transmitted in the network. The bar graph clearly shows that the proposed hybrid security model has improved the packet communication over the network effectively.
Figure 5: Remaining Energy Analysis

Another parameter defined to analyse the network reliability is the remaining energy in the network. The remaining energy defines the future chances of the network to perform. Only a node having energy can participate in the network. Initially, the network energy assigned in both existing and proposed architecture is same. But in existing approach, the network construction, security aspect, cluster switching, network communication and communication failure increased the communication loss. The Figure 5 is showing the high energy that loss occurs in the existing approach because of an unstable network and non-handling of network security. In this figure, x axis shows the communication rounds and y axis shows the network energy. The comparative bar graph shows that the network energy in proposed hybrid security model is much more than existing security model. It shows that the network reliability is improved in this proposed approach.

The results presented till now are taken on different time instances or rounds for a single network with 100 WBANs. To verify the significance of proposed hybrid security model, the simulation is applied on four different networks with 10, 20, 50 and 100 nodes. The scalability robust results are derived in terms of dead node, packet communication and network life. These results are able to verify that the network model is effective on larger as well as smaller networks. The simulation results are recorded by performing the communication for 2000 rounds for each network under existing and proposed security model.
The occurrence of dead nodes in a network affects the network communication behaviour, reliability and life. Higher, the dead nodes in the network more are the chances of failure occurrence. The path generation is also difficult in such network. Figure 6 is showing the comparative analysis of proposed security model for clustered network in terms of number of dead nodes occurred when the communication is performed for 2000 rounds on a network. The comparative results show that for 2000 rounds no node is dead in proposed approach when 10 and 20 nodes are taken. This shows that the existing approach is not effective in such scattered network. In the larger networks of 50 and 100 nodes, the numbers of dead nodes are much more than proposed approach in existing security model. It shows the proposed security model is robust and reliable than existing security model.

Figure 6: Scalability based Dead Node Analysis

Figure 7: Scalability based Packet Communication Analysis
Each of the nodes having sufficient energy can participate in packet communication in clustered network. The successful packet communication is the main objective of WBAN network. The existence of alive neighbour and controller nodes and the prevention from any attack increases the communication throughput. The packet communication based analysis results for different networks is shown in Figure 7. The bars in this figure shows that packet communication performed in case of existing secure WBAN and proposed hybrid security model. The comparative results show that the proposed security model has improved the network reliability and improved the packet communication over the network.

![Scalability based Network Energy Analysis](image)

**Figure 8: Scalability based Network Energy Analysis**

A node or network is called active, till it is having some amount of energy. Only an energy node can participate in the communication. The network life and packet communication depends on the energy of the network. In Figure 8, the comparative observations are provided in terms of network energy for different size clustered WBAN networks. The comparative results show that the remaining energy in case of proposed hybrid security model is higher than existing model. The stable network formation, preventive network communication and authenticated and encoded communication have improved the energy utilization and overall network life is improved.
IV. Conclusion

The distributed WBAN network suffers from various kinds of security attacks that can be performed by internal and external attacks. In case of clustered architecture, the communication is performed at multiple levels and the selection of controller and intermediate nodes is completely dynamic. This kind of architecture affects the network security and can result in heavy communication loss and performance degradation. In this paper, a hybrid security model is presented for stable and balanced clustered network. The security in this paper is achieved at identity level and message level. The node-to-controller and controller-to-controller communication is enabled through security integration. To achieve these security levels RSA and hashing methods are integrated with specific role. To integrate this security, the clustered network is generated based on energy, load and network constraint observations. The simulation of this security model is done on multiple clustered networks with 10, 20, 50 and 100 WBANs. The comparative analysis is done to evaluate the network reliability and performance in terms of dead node analysis, packet communication and network energy observation. The simulation results show that the proposed security model has effectively improved the network life and communication.

References


