CHAPTER 6

RESULTS AND DISCUSSION

6.1. INTRODUCTION

Remote health monitoring is going to be the way for the fast-paced gen Y and Z. A Body Area Network is a wireless network of health monitoring sensors designed to deliver individualized and remote healthcare. This piece of research till now expressed the developmental side of the novel scheme. This chapter is devoted to evaluate the effectiveness of the proposed research methodologies namely ECC with the FO signcryption, ARSS, and CP-HARS using matrix laboratory (MATLAB 12) – a proprietary programming language developed by MathWorks. MATLAB is a multi-paradigm numerical computing environment and fourth-generation programming language.

MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, Fortran and Python. Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing abilities. An additional package, Simulink, adds graphical multi-domain simulation and model-based design for dynamic and embedded systems.

The proposed research methodologies are compared with each other for evaluating the performance improvement. The simulation specific parameters are tabulated in table 6.1.

Table 6.1 SIMULATION PARAMETERS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>100*100</td>
</tr>
<tr>
<td>Nodes number</td>
<td>100</td>
</tr>
<tr>
<td>Initial energy</td>
<td>0.5J</td>
</tr>
<tr>
<td>BS location</td>
<td>(50,50)</td>
</tr>
<tr>
<td>Packet size</td>
<td>4000bits</td>
</tr>
<tr>
<td>E</td>
<td>50nJ/bit</td>
</tr>
<tr>
<td>ε_{fs}</td>
<td>10pJ/bit/m2</td>
</tr>
<tr>
<td>ε_{mp}</td>
<td>0.0013pJ/bit</td>
</tr>
</tbody>
</table>
The performance measure values which are taken into consideration in this technical work for the assessment of the enhancement of the newly introduced research technique. To evaluate the performance of the proposed approaches, several parameters are used as such as Message Size, Communication Overhead, Energy Consumption on Communication, and Computational Cost.

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. A comprehensive quantitative performance analysis is presented in this section. The energy consumption while message transmission and computation cost are the principle concerns of this section. The size of the message being transmitted is analyzed, in which the energy consumption related directly with the message size.

6.1.1. MESSAGE SIZE

If sentences are too long, it would not be easy to read and comprehend. When people communicate with each other, the messages that they send are usually broken into smaller parts or sentences. These sentences are limited in size to what the receiving person can process at one time. An individual conversation may be made up of many smaller sentences to ensure that each part of the message is received and understood.

Likewise, when a long message is sent from one host to another over a network, it is necessary to break the message into smaller pieces. The rules that govern the size of the pieces, or frames, communicated across the network are very strict. They can also be different, depending on the channel used. Frames that are too long or too short are not delivered.

The size restrictions of frames require the source host to break a long message into individual pieces that meet both the minimum and maximum size requirements. Each piece is encapsulated in a separate frame with the address information, and is sent over the network. At the receiving host, the messages are de-encapsulated and put back together to be processed and interpreted.

The size of the complete cipher text is computed in this scheme. The cipher text is the concatenation of time, message and attributes. Figure 6.1 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 Figure 6.1.

![Figure 6.1 MESSAGE SIZE VS. NUMBER OF USERS](image)

Figure 6.1 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 has achieved high level of security as compared to the existing ARSS and ECC with FO signcryption schemes.
6.1.2. COMMUNICATION OVERHEAD

In the field of computer science, overhead denotes any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal. It is a special case of engineering overhead. Sending a payload of data (reliably) over a communications network requires sending more than just the desired payload data itself. It also involves sending various controls and signalling data (TCP) required achieving the reliable transmission of the desired data in question. The control signalling is overhead. A simplified version is the need and time to dial a number to establish a phone call, before the call can take place. Dialling the number and establishing the call are overhead. Another simplified scenario is in the use of 2-way (but half-duplex) radios. Overhead would be the use of “over” and other signalling needed to avoid collisions, as extra traffic to that of the actual message(s) to be conveyed.

From the point concerns 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 I respectively. The relationship between the security level and communication overhead is represented in Figure 6.3. The communication overhead for the proposed CP-HARS increased along with the security level.

![Graph showing communication overhead vs. security level for ECC with FO signencryption, ARSS, and CP-HARS.](image)

**Figure 6.3 THE COMMUNICATION OVERHEAD VS. SECURITY LEVEL**

### 6.1.3. ENERGY CONSUMPTION ON COMMUNICATION

The energy consumption of Signcryption in CP-HARS is calculated from the formula $E=U*I*T$, 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 the 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 had significantly lesser energy consumption.

The results provided a very satisfactory argument in favour of CP-HARS. Also it is presumed that CP-HARS could execute a number of key exchange operations based on assumed battery life. Figure 6.4 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 schemes.

![Energy Consumption Graph]

**Figure 6.4 ENERGY CONSUMPTION ON COMMUNICATIONS WITH RESPECT TO THE NUMBER OF USERS**

### 6.1.4. COMPUTATIONAL COST

Computational complexity is a computer science concept that focuses on the amount of computing resources needed for particular kinds of tasks. In computational complexity theory, researchers assess the kinds of resources that will be needed for a given type or class of task in order to classify different kinds of tasks into various levels of complexity.

The cost of computation is the time taken by the computation and the cost of the hardware used for the computation. Figure 6.5 demonstrates the computational cost of ARSS signcryption with other schemes. The observation can be interpreted as follows: the computational cost of signcryption is lesser initially when compared to the other schemes. Energy consumption while performing communication and computation is considered inclusively.
Figure 6.5 COMPUTATION COST VS. THE NUMBER OF USERS

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 computational cost compare than the existing ARSS and ECC with FO signcryption schemes.

6.2. SUMMARY

In this chapter, a comprehensive comparative evaluation of the proposed research methodologies was done in terms of different performance metrics in the MATLAB simulation environment. The evaluation of the proposed research work proves to provide an effective and efficient developmental alternative to the existing methodologies. The research have paved for the development of hierarchical attribute-based ring signcryption to enhance security and privacy in Body Area Networks - a much needed technology in order deliver efficient health care delivery.