http://dx.doi.org/10.21172/ijiet.123.01

# Deployment Of Elliptic Curve Cryptography (Ecc) To Enhance Message Integrity In Wireless Body Area Network

Dr.Ahmad Alzubi[1], Abeer Sobkha[2]
[1,2]*Department of Management Information Systems,*
*University of Mediterranean Karpasia, Northern Cyprus, via Mersin 10, Turkey*

**Abstract- A WBAN for medical environments observing comprises of various sensor nodes that can checking the vital data and report the patients' health state. These sensor nodes are arrangement set on the human body. This study proposed solution for path loss in WBAN environments by using encryption algorithm. The Elliptic curve cryptography (ECC) is a way to deal with open key cryptography in view of the logarithmic structure of elliptic bends over limited fields. In this study we use the ECC technique to decrypt the patient's information before sending toreceiver station Furthermore,. the proposed solution approach shows that the number of iterations is not the mainfactor in obtaining the best schedule. We measure the path loss factor with Parameters of path loss models for MICS, 600, and 900 MHz, 2.4GHz and UWB band and by utilizing vector system analyzer. The perplexing path loss reaction was computed from the deliberate complex move capacity in the recurrence space by proposed method capacity of the instrument.**
**Keywords: Medical environments;path loss; encryption; WBAN security; ECC; sensors;cryptography.**

## I. INTRODUCTION

Path loss in wireless body area WBAN take a big attention in research area because the patients live depending this information, for that this study proposed method depending the Elliptic curve cryptography (ECC) to encrypt the data of patient before sending to the receiver station. ECC requires littler keys contrasted with non-ECC cryptography (taking into account plain Galois fields) to give proportional security. Elliptic bends are relevant for encryption, computerized marks, pseudo-arbitrary generators and different errands [1]. They are additionally utilized as a part of a few whole number factorization calculations that have applications in cryptography, for example, Lenstra elliptic bend factorization [2].The accurate area and connection of the sensor nodes on the human body rely on upon the sensor sort, size, furthermore, weight. Sensors can be worn as stand-alone gadgets or can be incorporated with gems, connected as small fixes on the skin, covered up in the client's garments or shoes, or even embedded in the client's body [3].The principle distinction amongst RSA and Elliptic Curve Cryptography is that not at all like RSA, Elliptic Curve Cryptography offers the same level of security for little key sizes. Elliptic Curve Cryptography is exceptionally scientific in nature. While routine open key cryptosystems (RSA, Diffie - Hellman and DSA) work specifically on extensive whole numbers, an Elliptic Curve Cryptography works over focuses on an elliptic bend [4].

The fig.1 Demonstrates a progressive model of Elliptic Curve Cryptography. Elliptic Curve Cryptography is isolated into three sorts of fields [5]. Field over genuine numbers, field over prime numbers, and a paired Galois field. The fundamental operations in Elliptic Curve Cryptography are Point Multiplication, Point Expansion and Point Doubling. These operations can be performed over a wide range of fields, be that as it may this usage bargains just with the prime field, which is more qualified for programming execution purposes [6].

<table>
<tr><td colspan="3">Elliptic Curve Cryptography</td></tr>
<tr><td colspan="3">Fields</td></tr>
<tr><td>Real Number Field</td><td>Prime Number</td><td>2^m Galois Field</td></tr>
<tr><td>Point addition</td><td>Point multiplication</td><td>Point Doubling</td></tr>
<tr><td colspan="3">Cryptography Algorithm</td></tr>
</table>

Figure1. Hierarchical Elliptic Curve Cryptography Model

## II. BACKGROUND OF THE STUDY

WBAN is extraordinarily impacted by the measure ofway misfortune that happens because of various weaknesse.

Path loss for WBAN are by and large set inside or on the body surface, in this way, misfortunes between these gadgets would influence the correspondence and can corrupt the execution observing in UHC [7,8]. In the taking after areas, we examine in insight about WBAN correspondence and way misfortune that happens in it and how it influences the execution of UHC [9]. Diminishment in force thickness of an electromagnetic wave presents way misfortune [10]. Path loss is for the most part brought on by free space disabilities of engendering sign like refraction, weakening, assimilation what's more, reflection and so on. It likewise relies on upon the separation amongst transmitter and beneficiary radio wires, the stature and area of reception apparatuses, proliferation medium, for example, wet or dry air and so on, and environment around the reception apparatuses like provincial and urban and so forth [11]. Path loss for WBAN is not the same as customary remote correspondence since it
relies on upon both separation and recurrence. Recurrence is provided food since body tissues are significantly influenced by the recurrence on which sensor gadget is working [12]. A typical of the mill topology of WBANs incorporates different sorts of restorative sensors that can be remotely associated to other restorative sensors or to the control hubs (e.g., PDAs), which could interface with different sorts of systems, for example, WiMAX or WiFI to facilitate convey the gathered medicinal data to the data focus [13]. Much incredible exertion has been given to create secure correspondence plans between the web and control hubs [14]. Therefore, our studies concentrate on the securing entomb sensor correspondence over the body range. In WBAN [15], key circulation is constantly defenseless against man in the middle assault. The dangers can be classified: Active assault and detached assault. The dynamic assailants can ready to drop messages and replay old messages, change messages. The detached assailants fit for listening the correspondence over WBAN [16].
Cipher technic like ECC is used to protect the patient information from attack or any changeduring transfer, the method by based encryption algorithm intended for asset obliged gadgets. Murmuring flying creature is an ultra-lightweight cryptographic primitive for encryption and validation in extremely asset compelled situations. We propose an ECG-Humming winged animal plan for secure correspondence over WBAN.

*2.1 Objective of study*

The goal of this study is solve the problem of path loss by using use ECC algorithm to improve the guarantee of send and receive information patient in medical area. Message Integrity, even though received messages are authenticated and encrypted, an adversary can intentionally tamper with the message. In such cases the receiving node should be able to detect such data corruptions and reject the message. Data can also get corrupted due to bad physical conditions of the wireless channel. A common way to deal with message integrity is give identification with description for every sensor node; the proposed algorithm implements the following Three modules: Routing Table, error Detector, and Path Selector.

*2.2 Research Methodology*

In this study proposed a new routing protocols to prove the send and receive patients' information in WBAN depending the research methodology that is used in this study as a way of achieving thesis objectives. The structure of the new technique is that it will improve the efficiency when used as perfect solution routing protocol which is proposed in an automated way to integrity sensed data, that’s by giving identification with description about the data and function for every node. Identification _ key technique is designed using the short description based on protocol index.
To evaluate the propsed technique, the study depends on testing the new algorithms by implementing the following three modules: Routing Table Constructor. Error Detector, and Path Selector.
transmits a broadcast message with identity to all the nodes to construct the routing table, each node that receives the message executes the Routing Table Constructor module to build its routing table. A node transmits data to the coordinator using the Path Selector module. The error Detector module detects whether or not this node is faulty. A node is considered faulty if it experiences congestion or when missing the identification key, a partial link problem, or a breakdown. If the node is found to be faulty, a message is sent to its neighbor nodes so that they can avoid this node during data transmission. The ECC help node to choose the nearest neighbor.

| Identity | Cost | Energy | Level | Flag |
|---|---|---|---|---|

Figure2. The id field represents identity sensor.

The routing table for a node has five fields as shown in Figure 2 The id field represents identity sensor. The cost field indicates the communication cost, i.e., the routing metric, for the path from this node to the coordinator. The level field indicates the level of the device and is different based on the characteristic of the node. The energy field represents the residual energy of the node and the flag field is a Boolean value representing whether or not a path

contains faulty nodes. Each node records information of neighbor nodes in its routing table based on the broadcast message from the coordinator.

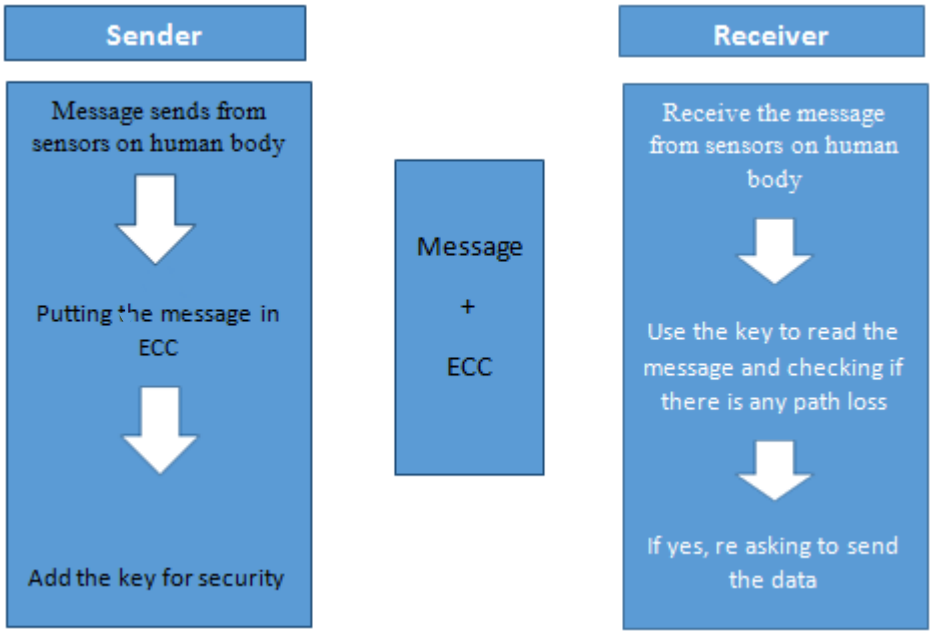


Figure 3. the main diagram of proposed model

## III. THE MEASUREMENT ENVIRONMENT

This study depend two scenario and measurements the vital patient data by using some parameters in addition to test the transition data by using some WBAN band wave. the measurements are done in emergency room hospital environment; Figure 3 indicates positions where the sensors nodes putting on the human body. the different between the first scenario and second scenario is the number of receiver station in addition both scenario test by ECC curve encryption. Adding a security layer to message integrity technique to prove the efficiency of message integrity in WBAN; we give the solution for the loss of messages and the change of the message through transfer between sender point and receiver point. That's mean currently the receiver device receiving data does not match with the data sent by patient sensor, this normally occurs because of the bad physical environment, type of wave transmission and the confusion. In the proposed method using MICS band to prove the Message Authentication, beside that using the checking factor of path loss, it'sa specific method for calculating a message authentication involving a cryptographic ECC in combination with a secret key. The proposed depending the path loss factor to get the result of simulation in both scenario, the different the two scenario is the number of receiver stations.

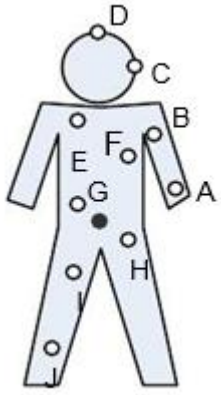


Figure 4. the points of sensors node on human body

In this estimation we use some devices according to some study [17,18] prove the efficiency of us it in different experiments. The path loss model is basically composed as
takes after:

$$L_{path}(d) = a \cdot \log_{10} d + [dB] b + N \quad (1)$$

where L path(d) implies the way misfortune in dB at a separation b mm. an and b signify parametersdetermined by a minimum square fitting to the deliberate normal way misfortune over the recurrence range,
l pathp j(d) which is given by

$$l_{path}(dlog)pj = -10 \cdot \frac{1}{N_F} \sum_{m=1}^{N_F} PL_p(f_m)_j [dB] \quad (2)$$

where fm remains for a recurrence which relates to the mthtest point at the estimation. In Eq. (2), N is a stochastic term which has a log-typical dispersion with zero-mean and standard deviation ofσN.

## IV. ENCRYPTION AND DECRYPTION PATIENT MESSAGE IN ECC

Elliptic Curve Cryptography is such a great decision for doing lopsided cryptography in versatile, essentially compelled gadgets at this moment, primarily in view of the level of security offered for littler key sizes. A popular, prescribed RSA key size for most applications is 2,048 bits. For comparable security utilizing Elliptic Curve Cryptography, you require a key size of 224 bits. The contrast turns out to be increasingly proclaimed as security levels increment (and, as a culmination, as equipment gets speedier, and the suggested key sizes must be expanded). A 384 - bit Elliptic Curve Cryptography key matches a 7680-piece RSA key for security.
The littler Elliptic Curve Cryptography keys mean the cryptographic operations that must be performed by the imparting gadgets can be pressed into significantly littler equipment, that programming applications may finish cryptographic operations with less processor cycles, and operations can be played out that much speedier, while as yet ensuring comparable security. That is to say, thus, less warmth, less power utilization, less genuine domain expended on the printed circuit board, and programming applications that run all the more quickly and make lower memory requests. Driving thus to more versatile gadgets which run longer, and create less warmth.
In our proposed method the using of Elliptic Curve Cryptography keys present in the side of sender and receiver, that's by using secret key in patient's sensors to decrypt the patient data before send to receiver station like use the value X and sends the public value g xmod p to receiver station. The receiver station chooses the secret value y and sends the public value g ymod p to sender station; the receiver station uses the value gxymodpas the secret key for confidential communications with receiver station.
Receiver station uses the value g yx mod p as the secret key. That's why g xy mod psame value of g yxmod p,the sensors patient and receiver station can use their secret keys with identification to send data between both stations in emergency room.
The algorithm of proposed solution programming in math lab environments, the simulation with the scenarios also in math lab. The proposed algorithm starts with reading the patients information then checking if there is any loss data by depending the table information then encrypt the data once by using ECC encryption algorithm.

### *4.1 The Simulation*

The first and second scenario uses four sensors around the human body, send data through the MICS band at 400 MHz to PC in the monitoring room. The steps of running as below: 1-collect data from sensors around the body, there is four sensors in different place (the figure below show the position of the sensors)
2- Send by MICS band to PC (in this scenario there is one receiver station).
3-checking the path loss, according the path loss factor
4-using a ECC in checking step (putting information in a table), if the path loss rescuing the data from sensors.
5-the receiver station receive is one in the first scenario and two in the second scenario.
The figure 4 and 5 show the first and second scenario environment.
The main elements of simulation are:
1-computer

2-phones
3-human body
4-sensors
5-mathlab programming software
6-wireless network

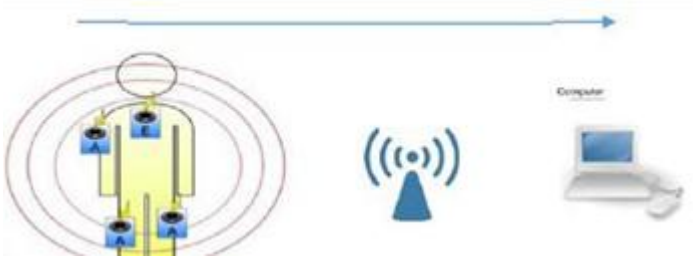

Figure 5. The first scenario (MICS Band 402-405MHz)


Figure 6. The second scenario (MICS Band 402-405MHz)

*4.2 The Analysis of Result*

The parameters for the path loss model, which are gotten from the deliberate information, are shown in Table 2.

TABLE 1 - PARAMETERS OF PATH LOSS MODELS FOR MICS, 600, AND 900 MHZ, 2.4GHZ AND UWB BAND

(a) Hospital room

| Parameters | Values | | | | |
|---|---|---|---|---|---|
| | MICS MHz | 600 MHz | 900 MHz | 2.4 GHz | UWB |
| a | 5.13 | 15.5 | 16.2 | 7.84 | 19.8 |
| b | 29.6 | 3.08 | 4.27 | 34.1 | 5.97 |
| σ N | 5.49 | 6.56 | 5.55 | 3.98 | 4.17 |

(b) Anechoic chamber

| Parameters | Values | | | | |
|---|---|---|---|---|---|
| | MICS MHz | 600 MHz | 900 MHz | 2.4 GHz | UWB |
| a | 24.5 | 17.4 | 28.4 | 30.0 | 44.9 |
| b | -14.8 | 1.24 | -22.6 | -18.3 | -54.5 |
| σ N | 5.64 | 7.02 | 11.7 | 7.02 | 3.22 |

The result of simulation depending the parameters of path loss in both scenario, the compare between before and after using the proposed method can see in figure 5, the figure (a) show the first scenario before using the propose method under normal condition and the figure (b) show same scenario after using the proposed algorithm. In figure (c) the second scenario in normal condition without using the proposed method, in figure (d) the same scenario under our proposed algorithm. These results we depending the path loss equation to measurement the path loss value.

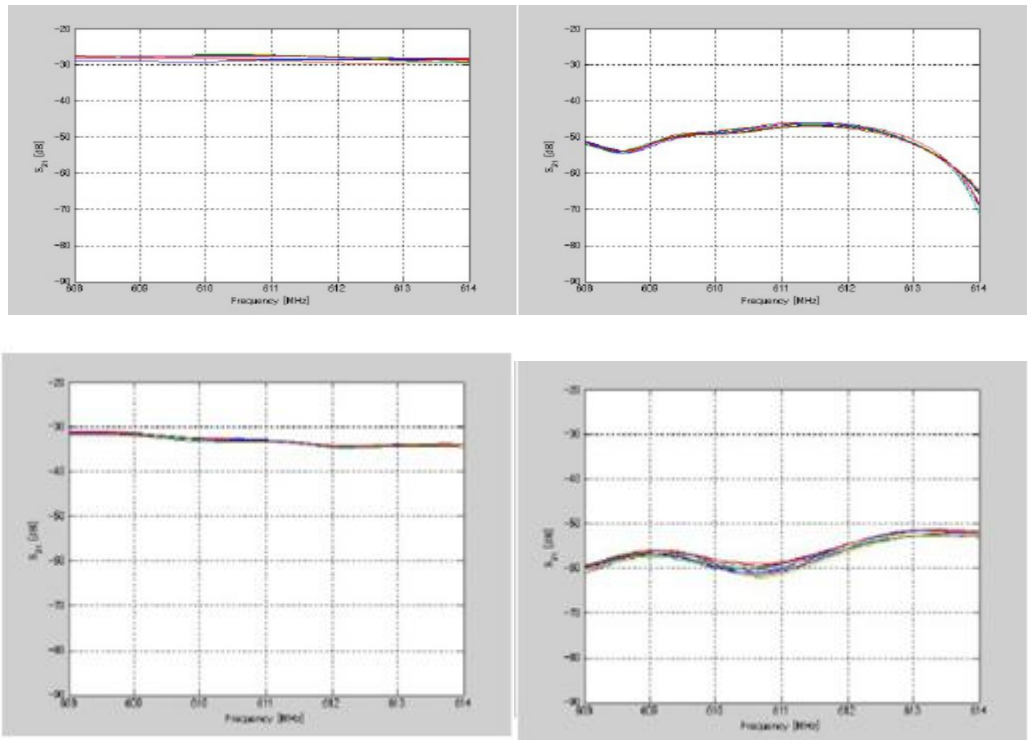

Figure 7. a) The first scenario before the propesed algoarithm (b) The first scenario after the propsed algorithm c) The second scenario before the propesed algoarithm (d) The second scenario after the propesed algoarithm

## IV. CONCLUSION

This study has discussed the performance of the first scenario approach in our proposed solution of path loss in WBAN environment. The result shows that the decrease of value of path loss after apply the identification key algorithm that's because the encryption level that was added to our technique, the approach is suitable to be utilized in medical device and health care environment with an added-on mathematical approach definingpath loss function in order to improve the MICS band performance in producing the best WBAN protocol. The result of the firs scenario obtained indicates the production of apatient's information during transfer between sensors nodes on human body and receiver station. It is being approved with using the ECC cipher function to get the security level in transfer area. simulation test that accepted the path loss where there is no significant difference between the schedule generated from scenario before using the proposed method and thescenario after using the proposed method. In addition, the result generated in some parameters was always connected with the previous value to make sure the weightage of each node sensor can be controlled. Furthermore, theproposed solution approach shows that the number of iterations is not the main factor in obtaining the best schedule.

We measure the path loss factor by using Parameters of pathloss models for MICS, 600, and 900 MHz, 2.4GHz and UWB band. The perplexing path loss reaction was computed from the deliberate complex move capacity in the recurrence space by proposed method capacity of the instrument.

## V REFERENCES

[1] Saisanathkumar, K., Reddy, K. N. K., Pushpavathy, V., & Reddy, P. R. (2016). Calculation of Path Losses at CM3 for Wireless Body Area Networks ( WBAN ) by using Different Types of Antennas, 11(7), 5210–5217.

[2] Ahmed, A. L. I., Ibraheem, Y., Safaai-jazi, A., Reed, J. H., Kohler, W. E., &Attiya, A. M. (2014). Implanted Antennas and Intra-Body Propagation Channel for Wireless Body Area Network

[3] Jaff, B. T. H. (2009). A Wireless Body Area Network System for Monitoring Physical Activities and Health-Status via the Internet, (March).

[4] Bh, P., Chandravathi, D., &Roja, P. P. (2010). Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz ' s Method, 02(05), 1904–1907.

[5] Conference, I., & Technology, I. (2005). IMPLEMENTATION OF ElGamal ELLIPTIC CURVE CRYPTOGRAPHY, (Icici), 1–6.

[6] Javaid, N., Khan, N. A., Shakir, M., Khan, M. A., Bouk, S. H., & Khan, Z. A. (n.d.). Ubiquitous HealthCare in Wireless Body Area Networks - A Survey.

[7] Khan, J. Y., Yuce, M. R., &Karami, F. (n.d.). Performance Evaluation of a Wireless Body Area Sensor Network for Remote Patient Monitoring.

[8] Kim, B., Cho, J., Kim, D., & Lee, B. (n.d.). ACESS : Adaptive Channel Estimation and Selection Scheme for Coexistence Mitigation in WBANs Categories and Subject Descriptors.
[9] Kp, C. E. Q. (2012). Elliptic Curve Cryptographic Algorithm, 978–981. http://doi.org/10.3850/978-981-07-1403-1
[10] Liu, D., Geng, Y., Liu, G., Zhou, M., &Pahlavan, K. (n.d.). WBANs-Spa : An Energy Efficient Relay Algorithm for Wireless Capsule Endoscopy, 1–5.
[11] Singh, V. (2013). Performanance Analysis of Mac Protocols for WBAN on Varying Transmitted Output Power of Nodes, 67(7), 32–34.
[12] Song, Y. (2010). Ultra Low Power Receiver Front end for WBAN Applications.
[13] Taparugssanagorn, A., Rabbachin, A., &Matti, H. (n.d.). A Review of Channel Modelling for Wireless Body Area Network in Wireless Medical Communications.
[14] Song, Y. (2010). Ultra Low Power Receiver Front end for WBAN Applications.
[15] J. Abouei, J. D. Brown, K. N. Plataniotis, and S. Pasupathy, "On the energy efficiency of LT codes in proactive wireless sensor networks," to
[16] appear in IEEE Transactions on Signal Processing, 2011.
[17] Singh, V. (2013). Performanance Analysis of Mac Protocols for WBAN on Varying Transmitted Output Power of Nodes, 67(7), 32–34.
[18] Tauqir, Anum, Nadeem Javaid, S. Akram, A. Rao, and S. N. Mohammad. "Distance aware relaying energy-efficient: Dare to monitor patients in multi-hop body area sensor networks." In Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013
[19] EighthInternational Conference on, pp. 206-213. IEEE, 2013.
[20] Geng, Yishuang, Yadong Wan, Jie He, and KavehPahlavan. "An empirical channel model for the effect of human body on ray tracing." In Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on, pp. 47-52. IEEE, 2013.