ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Enhanced DNA Cryptography for Wireless Body Sensor Networks

Ali abo Ajeeb[1], Ahmad Mahmod[2], Boushra Maala[3], Ahmad S. Ahmad[4]

Fourth Year Student, Department of Medical Engineering, Al-Andalus University, Alkadmous - Tartous, Syria[1]

Fourth Year Student, Department of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria[2]

Assistant Professor, Department of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria[3]

Assistant Professor, Department of Medical Engineering, Al-Andalus University, Alkadmous - Tartous, Syria[4]

ABSTRACT: A Wireless Body Sensor Network (WBSN), is a network of sensors that worn or deployed on a person's body. This network plays an important role in medical field, where it allocates the vital information from the body and transmit it wirelessly to a central station to process it.We need to provide security and privacy for sent data because of the sensitivity of this information. In this paper, we propose an enhanced DNA cryptography technique that depending on nucleotides relationship concept to generate a data encrypted stream represent the sensors allocated data, so the intruder will not be able to modify this data while he is not knowing the technique of encryption, which provides a secure and private data transmission.

KEYWORDS: Wireless Body Sensor Networks; Security; Cryptography; DNA Cryptography

I. INTRODUCTION

In the past years, the Wireless Sensor Networks (WSNs) have very great interest specially the Wireless Body Sensor Networks (WBSNs) that uses to allocate the vital information from the body. The main motivation is the enormous development in the field of tiny and intelligent electronics that known as micro-electronical systems "MEMS". Today, we can see medical body sensors which can worn on or implanted in the body. WBSNs today take an attractive attention of the researches working in the cryptography area [1][2].

From Fig.1, we can notice that the network consists of many nodes that related to each other's. When a node need to transmit any vital data, the data should transfer from a node to another one and so on, until this data arrives to the last node that transmit it to a Basic Station (BS) that in role transmit it to its destination that can be a hospital or a doctor clinic to process and analyse this data and take the appropriate procedure.

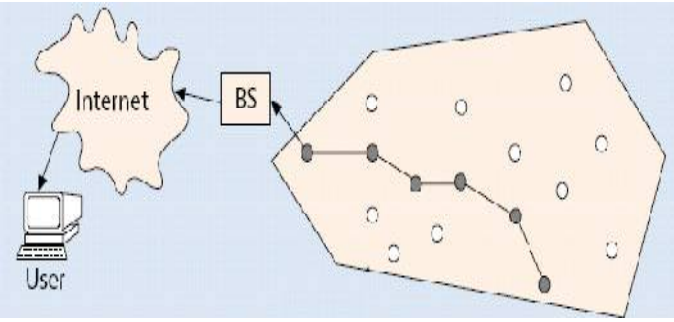

Fig.1. WBSN network

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

The WSNs in general have a limited capacity of storage, computing resources and battery power. So, when we aspire to secure the data, we should apply a cryptography algorithm that consume a little storage, power and memory as possible to increase the life span of the network, and ensure that every point in the network is safe [3].

In general, Body Sensor nodes have four main tasks, which are: signal detection, coding, digitizing and transmitting and receiving of data process. Also, they are responsible of amplification of the vital data because the allocated human body data is accompanied with noise [4].

WBSNs need to provide all the services of security like "confidentiality" that means hiding the data from unauthorized party, "authentication" to ensure the reliability of the message by identifying its origin, "integrity" to preventing the information from unauthorized modification and "availability" to ensure that services and information can be accessed at the time they are required [5].

In this paper, we will provide a security technique based on DNA cryptography that converts the patient information (name, ID, and medical state) to a cipher text to share it between the nodes and the central server. We apply a computational method depends on the relationship of nucleotides which means that the last form of the cipher text is similar to the way that nucleotides related with each other.

II. RELATED WORK

WBSN typically comprise sensor devices that worn or implanted with the body for measuring physiological data (vital signs, motion, …etc) [6]. WBSNs must transmit this data in a secure manner in order to ensure user's privacy. To achieve that, a robust encryption method should be applied. In this section we will discuss cryptography fundamental, DNA structure and DNA cryptography genesis.

A. *DNA (Deoxyribonucleic Acid):*

DNA is the hereditary material in humans and almost all other organisms, nearly every cell in a person's body has same DNA and most DNA is located in the cell nucleus (where is called nuclear DNA). DNA also has the capacity to perform calculations many times quicker than computers that we use in our world. It has the genetic instruction that needed to construct the other cells like RNA (Ribonucleic Acid) and protein. Simple operations (addition and subtraction) are applying to the initial data in DNA to construct a complex structure of human's body [7].

The information in DNA is stored as a code made up of four chemical bases: adenine (A), guanine (G), cytosine (C), and thymine (T). Figure.2 shows DNA's structure.

Fig. 2. DNA chemical bases

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

DNA pairs up with each other, (A with T) and (C with G), to form units called "bases pairs". Each base is also attached to a sugar molecule and phosphate molecule. Together, a base, sugar and phosphate are called a "nucleotide ".

Nucleotides are arranged in two long strands that form a spiral called a " double helix ". The structure of the double helix is somewhat like a ladder, with the base pairs forming the ladder's rungs and the sugar and phosphate molecules forming the vertical side pieces of the ladder [8].The structure of ladder is shown in Fig. 3.

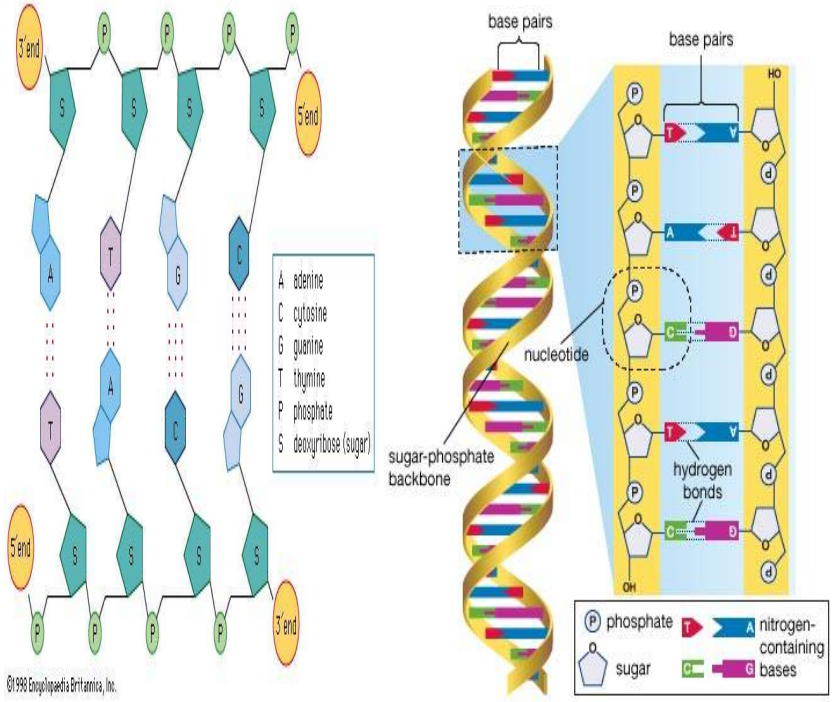

Fig.3. Ladder's structure (rungs and vertical)

B. *DNA Cryptography:*

DNA cryptography is a technique that depend on the DNA work principle to make a high level of security cipher text. Where, DNA is used as information carrier. The DNA cryptography was invented by Adelman in 1994 of University of Southern California, so this technique is a new development in the field of security.

The vast parallelism, very high energy efficiency and extraordinary information density that exist in DNA are being explored for computing, data storage and cryptography. So, this might lead to a new revolution information science.

Depending on the above, DNA cryptography is developed with research of DNA computing and the progress of electronic technology played a main role in this development. So, DNA cryptography becomes the most advanced technique in cryptography field [9].

III. PROPOSED ALGORITHM

A. *Overview:*

In our proposed cryptographic technique, we will generate the public and private keys for nodes depending on RSA algorithm and those keys will allocated to nodes before put them at work in order to save storage and power because of the limitation of these two parameters. Our method is named Enhanced DNA Cryptography for WBSN (EDNAC-WBSN).

We will distribute the keys between nodes in usage of the Secure Channel during the process of communication between nodes.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

B. *Description of the Proposed Algorithm (EDNAC-WBSN):*

Our proposed work enhanced the security by using eight pairs of characters (A, B, C, D, E, F, G, H) instead of the four (A, T, C, G) that DNA provides them. The reverse of the cipher text by replacing every character with its opposite character is another method to enhance the security.
The proposed cryptographic system converts every letter to a combination of characters that generated based on DNA. To more understand our idea, we will explain this technique with the following example:
We will suppose that we want to encrypt the " NODE " word. So, we will follow the next steps:

1- Firstly, we will convert every letter of the word to its numerical value from ASCII table. As the following:
N ="78", O ="79", D="68", E="69", where this numerical numbers are represented in Base-10
2- Now, we will convert every decimal value to its octal value as the following: N="116", O ="117", D="104", E="105".
3- We will encrypt this sequence with a public key using RSA that is 7-length, assume that key is (2 7 8 3 5 6 1), and by get the octal value for every decimal number, the key will be in its octal form (2 7 10 3 5 6 1).
4- The resulted sequence is (2 7 10 3 5 6 1 116 117 104 105), and based on DNA that provides four unique pairs by associated every nucleotide with its couple A with T and C with G (AT, TA, CG, GC). We can replace every octal value by its proposed pair, where we associated A with B, C with D, E with F and G with H. So, the resulted pairs that represent the alphabet for our cryptographic system are (AB, BA, CD, DC, EF, FE, GH, HG).
5- The proposed pairs for the octal values is:

0 → AB , 1 → BA
2 → CD , 3 → DC
4 → EF , 5 → FE
6 → GH , 7 → HG

So the resulted sequence is:

(CD HG BA AB DC FE GH BA BABA GH BA BA HG BA AB EF BA AB FE).

6- Now, we have a series of characters related with each other like a DNA cipher.
7- Finally, for more secure we will converse the result by replacing every character with its couple (A, B) (C.D) (E, F) (G, H). Then, we can get the final result in this form:

(DC GH AB BA CD EF HG AB ABAB HG AB AB GH AB BA FE AB BA EF).

and this based on DNA, where we can make a bond only between (A and T) and (C and G).

The legal node can extract the original data by using a reverse method that used in encryption. Where, we should reverse the received series and then replace every pair with its associated value. So, we have a resulted series with a Base-8 values. We should later convert every three values to its decimal value, and according to ASCII table we can get the appropriate letter for every value and finally we get original series.

IV. SIMULATION RESULTS

Fig.4 and Fig.5 show an encryption/decryption process using JAVA Programming Language.
In Fig.4, we can see how a sensor sends a word (NODE) "without a public key" that we take it in the example. We also notice the resulted data before and after reverse.
We notice from Fig.5 that the data that was encrypted (NODE) was extract again from its encrypted form. The most important is that it is very difficult to attackers to extracted the plain text if they do not know the technique of encryption step by step.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Fig.4: Encryption in EDNAC-WBSN

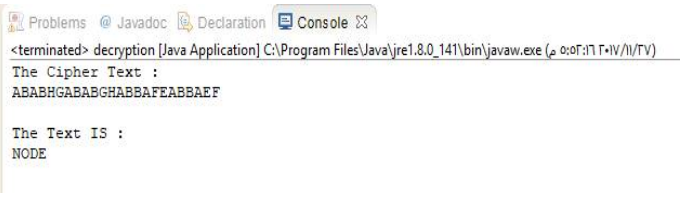

Fig.5: Decryption in EDNAC-WBSN

Finally, we present the proposed encryption technique by the following flowchart.

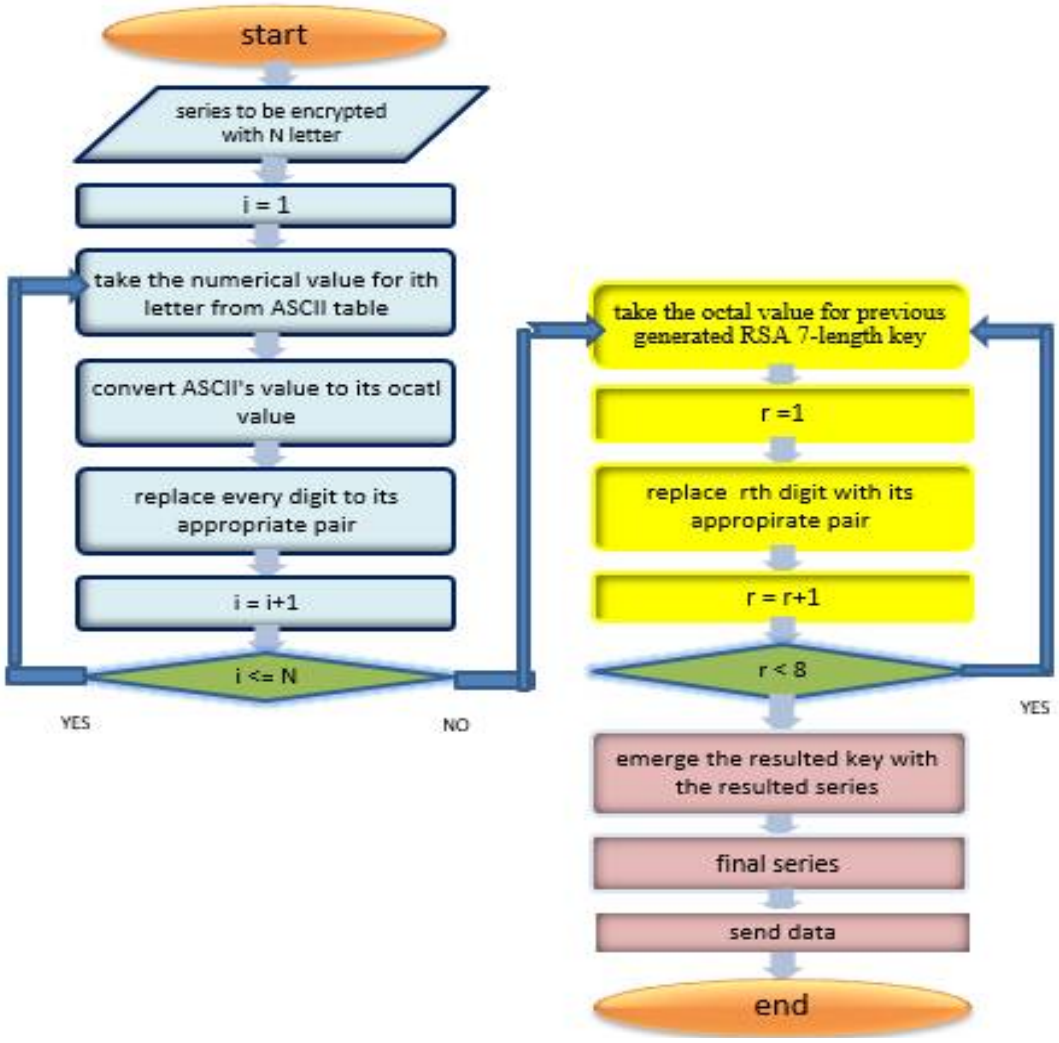

Fig.6: Flowchart for our proposed encryption method

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

V. CONCLUSION AND FUTURE WORK

In this paper, we proposed a secure cryptographical technique based on the concept of nucleotides in DNA named EDNAC-WBSN. We generated the public and private keys by using RSA and we distributed them on the Body Sensors using Secure Channel. After that, we saw the final output as a couples of characters that we have supposed them depending on ASCII table and Decimal and octal systems.
Our proposed technique was implemented in JAVA and we have obtained the desired results. As a future works, we will try to provide more secure and effective method in DNA cryptography field which increase the safety of WBSN.

REFERENCES

1. Monika Poriye and Shuchita Upadhyaya. "Improved Security using DNA Cryptography in Wireless Sensor Networks". International Journal of Computer Applications (0975 – 8887) Volume 155 – No.13, 2016.
2. Benoit Latre´, Bart Braem , Ingrid Moerman ,Chris Blondia and Piet Demeester. "A survey on wireless body area networks". Wireless Netw (2011) 17:1–18. DOI 10.1007/s11276-010-0252-4, 2011.
3. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci."Wireless sensor networks: a survey". Computer Networks 38 (2002) 393–422, 2002.
4. Aarti Sangwan and ParthaPratim Bhattacharya. "Wireless Body Sensor Networks: A Review". International Journal of Hybrid Information Technology 8(9) pp :105-120, 2015.
5. Madhumita Panda. "Security in Wireless Sensor Networks using Cryptographic Techniques". American Journal of Engineering Research (AJER) 3(1) pp:50-56, 2014.
6. Tuncer Can Aysal and Kenneth E. Barner. "Sensor Data Cryptography inWireless Sensor Networks". IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY 3(2), 2008.
7. S.Jeevidha, M.S.Saleem Basha and P.Dhavachelvan. "Analysis in DNA Based on Cryptography to Secure Data Transmission". International Journal of Computer Applications (0975 – 8887) Volume 29– No.8, 2011.
8. M.Borda, and O.Tornea, "DNA secret writing techniques". Communications (COMM), 8th International Conference on Bucharest (909 – 2007) pp: 451-456, 2010.
9. XIAO Guozenho, LU Mingxin, QIN Lei and LAI Xuejia. "New field of cryptography: DNA cryptography". Chinese Science Bulletin, 51(12):413—1420, 2006.
10. Shivani Sharma and Yash Gupta. "Study on Cryptography and Techniques". International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) 2(1) ISSN: 2456-3307, 2017.
11. MING LI and WEN JING LOU."Data Securityand PrivacyinWireless Body Area Networks". IEEE Wireless Communications 1536-1284/10, 2010.
12. Gurpreet Singh and Supriya. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security". International Journal of Computer Applications (0975 – 8887),2013.