# Improved Security using DNA Cryptography in Wireless Sensor Networks

Monika Poriye
Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, 136118, Haryana, India

Shuchita Upadhyaya
Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, 136118, Haryana, India

## ABSTRACT

Secure communication and data transmission is necessities in wireless sensor networks and security of sensitive data is the major concern in WSNs. DNA cryptography depicts a crucial part in the area of security. In DNA cryptography, DNA nucleotide bases are used to store huge amount of data. This paper includes a new security technique based on DNA concept that enhance the security of the wireless sensor networks by including false data in original data, which results a DNA sequence in terms of nucleotide bases. Therefore, intruders will not be able to acquire the main encoded information and encounter enough difficulties to cryptanalyst the coded message. This final data (cipher) consist of the extra information i.e. false information with the original message. It would be much difficult to amplify encoded message sequence by the intruder without knowing the correct sequence of cipher.

## General Terms

Security, Algorithms et. al.

## Keywords

DNA cryptography, Security, WSN, Encryption & Decryption

## 1. INTRODUCTION

In the past decade, WSNs have gained world-wide attraction due to the expansion in Micro-electromechanical systems (MEMS) technology. MEMS contain micro-circuitry on a tiny silicon chip which include fabricated sensor as a mechanical device, used for data collection in any environment. Wireless sensor networks have many applications like in military, hospitals, environment and seismic sensing etc. As WSN has wide range of application and have attracted attention of the researchers working in the area of cryptography. The sensor nodes have limited capacity of storage, battery power and computing resources when compared with traditional sensors [1]. WSNs have different number of security problems that become a challenging revaluation in many areas, comprising design of cryptographic techniques; how to get privacy, authentication, and integrity. Selecting an appropriate cryptographic algorithm for making a secure network is a vital task in wireless sensor networks. For making cryptographically secure network, security should be applied at each point of the network. As in WSN, cryptography depicted technique should be robust in nature and should not consume more memory, power & energy, so that the lifespan of the network can be increased [2] [3] and DNA cryptography is one of the emerging technique for sensor network security, which solves these problems. For secure message transmission, different DNA cryptographic methodologies are used like bio-molecular, polymerase chain reaction (PCR), and one-time-pad to encipher the data. Parallel processing capabilities are used for Bio molecular technique. PCR technique is based on DNA Digital coding; in which message are converted into binary code and then converted into DNA sequence that is the DNA nucleotide bases and One-time-pad technique is used to encode and decode messages [4].

Earlier studies [5,6] showed that it is feasible to apply DNA based algorithms for providing the high security in wireless sensor network as by applying traditional cryptography (like as DES, RSA), encoded data can be recognized by an attacker. DNA has the capacity to store large amount of information rather than existing algorithms. It is a new technology for unbroken data.

The overall aim of this paper is to provide a new security technique based on DNA cryptography which completely secures the data. Here, the information transferred to the other party is to be secured with the help of computation and biological based security (nucleotide bases). The final data is in the form of nucleotide bases which is then stored as a DNA sequence. Redundant data are generated and combined with the cipher text in order to make it more complex to the intruders. Thus it may confuse the attacker in identifying the original data.

To explore the security issues in WSN, DNA cryptography and their applicability is discussed in section 2. Section 3 describes the proposed scheme. Results are shown in section 4. Finally, section 5 concludes the paper.

## 2. RELATED WORK

Security is one of the most important and challenging problem in wireless sensor networks. Sensor networks need fundamental security services like authentication, integrity, privacy and non-repudiation. As sharing of information increases day by day through the network thereby increasing much of the risk of secure transmission over the sensor networks. In this section, discussion begins with the fundamental of cryptography and then enhancements are manifested.

### 2.1 Cryptography

Cryptography is the premise of security and due to the vast technologies coming these days, all the manual systems are converted into web applications. So, the sensitive data which is being transmitted over internet is unprotected as a consequence of many security attacks [7] [8]. Various cryptographic techniques have been used to acquire the security in wireless sensor networks [9] [10]. Encryption & decryption are the two main process of cryptography. Encryption is the process of concealing the data in such a way that the third party is not able to read it. Symmetric and asymmetric are different types of cryptographic techniques; Symmetric (private-key) cryptography uses only single key for encryption and decryption process. Data Encryption

Standard (DES) and Advanced Encryption Standard (AES) are the two main algorithms used for the symmetric key cryptography [11]. Asymmetric key cryptography, also known as public-key cryptography needs two keys to encode and decode the data. RSA (Ron Rivest, Adi Shamir, and Leonard Adleman) [12] and Elliptic Curve Cryptography (ECC) [13] are the main asymmetric algorithms.

Cryptanalysis works collateral with cryptography. The cryptanalyst always try to harm the security proposed by cryptography. In order to avoid the damage by cryptanalyst, it is necessary to design cryptographically secure system that provides high level of security in wireless sensor networks.

## 2.2 DNA

Deoxyribonucleic acid holds hereditary information of all living things and gives the genetic direction for building other cells [14] [15]. It is located in the nucleus as well in mitochondria. DNA is a double helix structure which carries the genetic information in two strands. The DNA structure is shown in Figure 1.

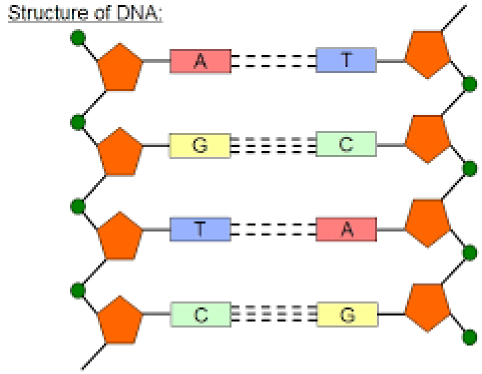


**Fig 1: DNA Structure**

DNA is made of four types of nucleotides: adenine (A), cytosine (C), guanine (G), or thymine (T). There is hydrogen bond present between base pairs [16]. These bases contains the information present in living being and these bases also make a sequence of triplet called a codon as shown in example (Figure 2).

Nucleobases makes the sentences known as genes. The genes lie in long strands of DNA called the chromosomes and contains information to form proteins. The combination of these nucleobases (genes) forms the different characterstics of humen being. The way in which the nucleotides bases are linked together with phosphate & sugar groups formed a DNA strand chemical polarity of 5' phosphate and 3' hydroxyl at top & bottom [17]. The structure shown in Figure 3.

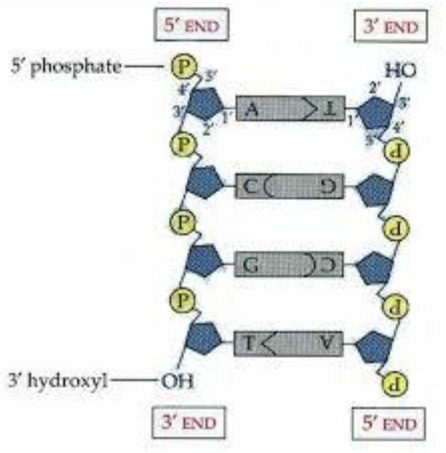


**Fig 3**

DNA has unique structure to perform biological function & thus solve the complex mathematical problems.

## 2.3 DNA Cryptography

DNA Cryptography is highly secure technique, in which DNA is used as information carrier. Due to extra ordinary information density inherent in DNA molecules DNA can be used for all sorts of cryptographic techniques [16].

DNA strands can be used to store information in terms of nucleotide bases [17]. Thus DNA Cryptography gives the high strength of security for storing sensitive information due to the usage of nucleotides which are unique for an organism. This cryptographic technique was invented by Adelman in 1994 of University of Southern California to give the solution of complex mathematical problems [18]. From the security point of view, DNA Cryptography is a new advancement in the field of security.

A mathematical computation is applied with DNA cryptography for providing it more powerful than the traditional cryptographic schemes [19].

# 3. PROPOSED WORK

To impart security in wireless sensor networks, the public & private key pairs are generated with the usage of RSA algorithm. As in WSN, the sensor nodes have the limitation of tiny storage & low power, so key pairs are allocated to the sensor nodes primarily before deploying them in any environment to save the energy of sensor nodes for generating keys. The process of distribution of key between sensor nodes is done through the secure channel (SSL) during communication process [19]. In the proposed system, security is enhanced with the use of false data inserted within the original data which are in the form of nucleotide bases. It is a Cryptographic based technique in which every letter of the alphabet is converted into a dissimilar combination of the four bases that may become the human DNA. The identification of even the existence of the encoded data is most unlikely.

DNA bases makes DNA strand

ATACCTTGATACCATGCAACCCGGTAA

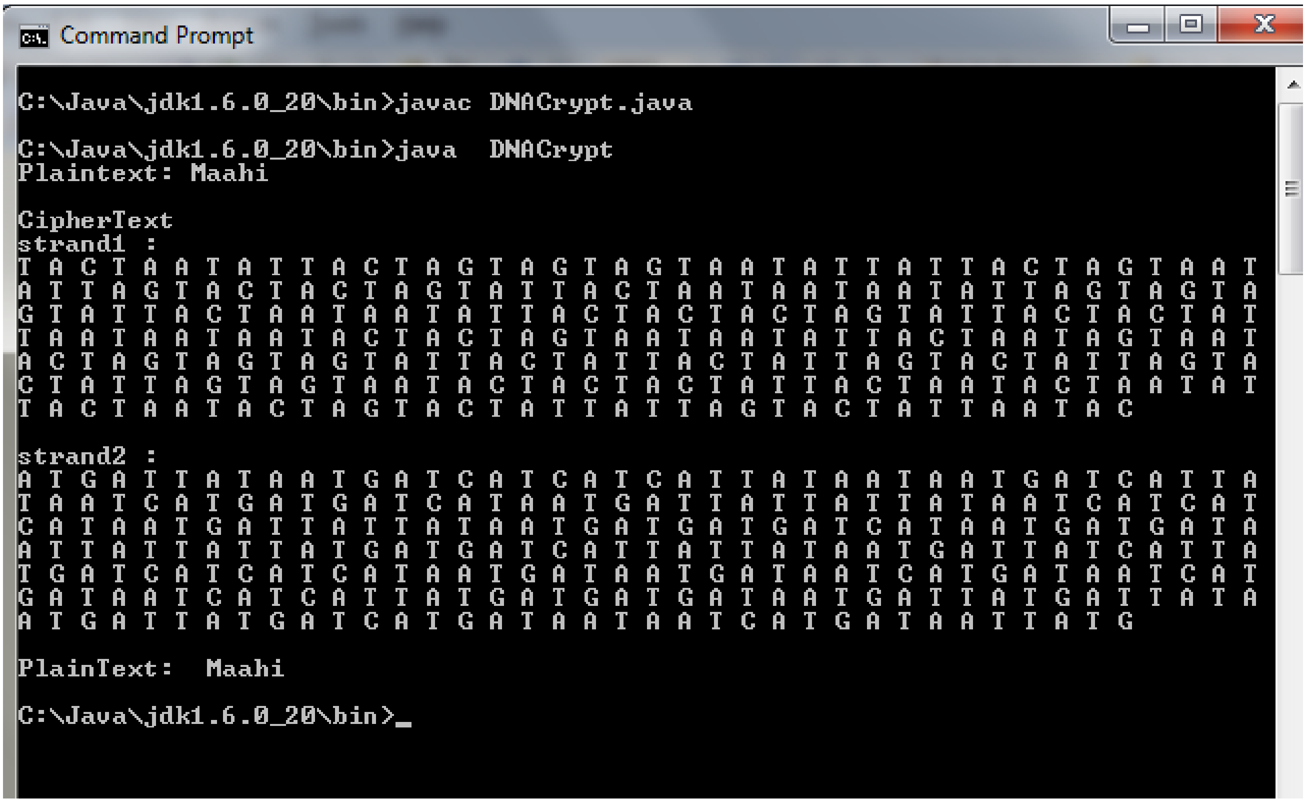
letters makes Codons (triplet word)

ATA CCT TGA TAC CAT GCA ACC CGG TAA

Words make sentences

ATA-CCT-TGA TAC-CAT-GCA ACC-CGG-TAA

Fig 2: Codon



```
C:\Java\jdk1.6.0_20\bin>javac DNACrypt.java

C:\Java\jdk1.6.0_20\bin>java  DNACrypt
Plaintext: Maahi

CipherText
strand1 :
T A C T A A T A T T A C T A G T A G T A G T A A T A T T A T T A C T A G T A A T
A T T A G T A C T A C T A G T A T T A C T A A T A A T A A T A T T A G T A G T A
G T A T T A C T A A T A A T A T T A C T A C T A C T A G T A T T A C T A C T A T
T A A T A A T A A T A C T A C T A G T A A T A A T A T T A C T A A T A G T A A T
A C T A G T A G T A G T A T T A C T A T T A C T A T T A G T A C T A T T A G T A
C T A T T A G T A G T A A T A C T A C T A C T A T T A C T A A T A C T A A T A T
T A C T A A T A C T A G T A C T A T T A T T A G T A C T A T T A A T A C

strand2 :
A T G A T T A T A A T G A T C A T C A T C A T T A T A A T A A T G A T C A T T A
T A A T C A T G A T G A T C A T A A T G A T T A T T A T T A T A A T C A T C A T
C A T A A T G A T T A T T A T A A T G A T G A T G A T C A T A A T G A T G A T A
A T T A T T A T T A T G A T G A T C A T T A T T A T A A T G A T T A T C A T T A
T G A T C A T C A T C A T A A T G A T A A T G A T A A T C A T G A T A A T C A T
G A T A A T C A T C A T T A T G A T G A T G A T A A T G A T T A T G A T T A T A
A T G A T T A T G A T C A T G A T A A T A A T C A T G A T A A T T A T G

PlainText:  Maahi

C:\Java\jdk1.6.0_20\bin>_
```

**Fig 4: Encryption/Decryption Process**

As an example, it is shown here how to convert the single letter "P" into DNA-ready code. Firstly the ASCII table converts the given letter of the plaintext to be encrypted into numerical value (i.e. P=80). The ASCII value that is generated is in Base 10 form. Further this ASCII value is encrypted with public key of sensor node which is 7(generated by using RSA) for getting mini cipher i.e. (20971520000000). After that, convert mini cipher into base-4 conversion which will transform the decimal form of output to the quaternary form (i.e. 1103302320020). Finally, numbers with 0, 1, 2, and 3 can be changed into their DNA base equivalents and are replaced with A, T, C, and G respectively. As an example "p" will become ACACAAATATAAAGATAGAAAAAGAA. This information is then blended with the false information generated computationally i.e. TGTGTTTATATTTCTATCTTTTTCTT, completely compatible to final cipher data meaning that the first letter of ciphertext is 'A' and similar compatible data generated is 'T', second letter is 'C' and equally false letter is 'G' and so on. Because in DNA, A can only make a bond with T, similarly C can only make a bond with G. To retrieve the data on the other end, the Decrypter would take the data in form of DNA sequence. The ciphertext are emerged from the false data and then the whole process is reversed to get the original plain text.

In Figure 4, an encryption/decryption process is performed in which original information is stored in terms of nucleotide bases. Here strand1 contains the true cipher and strand2 contains the unnecessary cipher data. Both data (true cipher & false cipher) merges in such a way that makes a complete form of DNA i.e. the first letter of strand1 is 'T' and equally generated a false data 'A' in strand2 and so on. The attackers will encounter enough problems to cryptanalyst the coded message because this ciphertext consists of extra information with the original message. It would be much difficult for the third party to decode the message sequence without knowing the exact sequence of cipher. Thus, this technique may create confusion for attacker to determine the original information.

## 4. CONCLUSION

In this paper, a secure method of DNA Cryptography using the concept of biological DNA has been proposed. Here, the key pairs are generated with the use of RSA algorithm and is distributed among sensor nodes by using SSL protocol. In the final step, the output shown in the form of nucleotide bases (A, C, G & T) which merges with false data for making confusion for the attacker. It may be anticipated that the usage of false data with original information may enhance the security against the negative parties in wireless sensor networks. The concept is implemented in java and desired results have been obtained.

## 5. REFERENCES

[1] Gilbert, E. P. K., Kaliaperumal, B. and Rajsingh, E. B. 2012 Research Issues in Wireless Sensor Network Applications: A Survey. International Journal of Information and Electronics Engineering. 2, 702-706. DOI: 10.7763/IJIEE.2012.V2.191.

[2] Pathan, A. S. K., Lee, H. W. and Hong, C. S. 2006. Security in Wireless Sensor Networks: Issues and Challenges. ICACT2006, 20-22. DOI: 10.1109/ICACT.2006.206151.

[3] Sharma, G., Bala, S. and Verma, A. K.2012. Security Frameworks for Wireless Sensor Networks-Review. Procedia Technology. 6, 978-987. http://dx.doi.org/10.1016/j.protcy.2012.10.119.

[4] Anwar, T., Paul, D. S. and Singh, S. K. 2014. Message Transmission Based on DNA Cryptography: Review. International Journal of Bio-Science and Bio-Technology, 6, 215-222. http://dx.doi.org/10.14257/ijbsbt.2014.6.5.22

[5] UbaidurRahman, N. H., Balamurugan, C. and Mariappan, R. 2015. A Novel DNA Computing Based Encryption and Decryption Algorithm. Procedia Computer Science, 46, 463 – 475. Doi:10.1016/j.procs.2015.02.045.

[6] Javheri, S. and Kulkarni, R. 2014. Secure Data communication and Cryptography based on DNA based Message Encoding. International Journal of Computer Applications. 98, 35-40. Doi:10.5120/17271-7733.

[7] Saini, N., Pandey,N. and Singh, A. P. 2015.Enhancement of security using cryptographic techniques. 4th International Conference on IEEE, (2015) 1-5. DOI: 10.1109/ICRITO.2015.7359224

[8] Galbreath, N. 2002. Cryptography for Internet and Database Applications: Developing Secret and Public Key Techniques with Java. New York, USA: John Wiley and Sons, Inc., 2002.

[9] Ren, X. 2006. Security Methods for Wireless Sensor Networks. Proceedings of the 2006 IEEE, International Conference on Mechatronics and Automation, 2006, Luoyang, China. 1925-1930.

[10] Sekhar, V. C. and Sarvabhatla, M. 2012. Security In Wireless Sensor Networks With Public Key Techniques. 2012 International Conference on Computer Communication and Informatics (ICCCI -2012), Jan. 10 – 12, 2012, Coimbatore, INDIA. 1-16.DOI: 10.1109/ICCCI.2012.6158861.

[11] Singh, G. and Supriya. 2013. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. International Journal of Computer Applications. 67, 33-38. DOI: 10.5120/11507-7224.

[12] Frunza, M. and Scripcariu, L. 2007. Improved RSA Encryption Algorithm for Increased Security of Wireless Networks. 2007 International Symposium on Signals, Circuits and Systems, Iasi. 1-4. doi: 10.1109/ISSCS.2007.4292737.

[13] Kodali,R. K. and Sarma, N. V. S. N. 2013. Energy efficient ECC encryption using ECDH. Emerging Research in Electronics, Computer Science and Technology,Lecture Notes in Electrical Engineering, Springer. 248, 471–478. DOI : 10.1007/978-81-322-1157-0_48.

[14] https://ghr.nlm.nih.gov/primer/basics/dna

[15] Mandge, T. and Choudhary, V. 2013. A DNA encryption technique based on matrix manipulation and secure key generation scheme. Information Communication and Embedded Systems (ICICES), 2013 International Conference on, Chennai. 47-52. doi: 10.1109/ICICES.2013.6508181.

[16] Borda, M. and Tornea, O. 2010.DNA secret writing techniques. Communications (COMM), 2010 8th International Conference on, Bucharest. 451-456. doi: 10.1109/ICCOMM.2010.5509086.

[17] https://www.ncbi.nlm.nih.gov/books/NBK26821/, Molecular Biology of the Cell. 4th edition.

[18] Pramanik, S. and Setua, S. K. 2012. DNA cryptography. Electrical & Computer Engineering (ICECE), 2012 7th International Conference on, Dhaka. 551-554. doi: 10.1109/ICECE.2012.6471609

[19] Watson,J. D. and Crick, F. H. C. 1953. Molecular structure of nucleic acids. Nature. 171.4356, 737-738. doi:10.1038/171737a0.

[20] Adelman, L. 1994. Molecular computation of solutions to combinatorial problems. Science in JSTOR. 266,1021–1025. DOI: 10.1126/science.7973651.

[21] Monika and Upadhyaya, S. 2015. Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks. 4th International Conference on Eco-friendly Computing and Communication Systems, Procedia Computer Science. 70, 808 – 813. doi: 10.1016/j.procs.2015.10.121.