International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Secure Data Communication Using DNA based Cryptography in Mobile Adhoc Network

Snehal Javheri[1], Rahul Kulkarni[2]

[1]Sinhgad Institute of Technology, Department of Computer Engineering,
Lonavala Pune. University of Pune, India

[2]Sinhgad Institute of Technology, Department of Computer Engineering,
Lonavala Pune. University of Pune, India

Abstract: ***DNA cryptography is a new promising direction in cryptography research that emerged with the evolution in DNA computing field. DNA can be used not only to store and transmit the information, but also to perform computation. The extensive parallelism and extraordinary information density inbuilt in this molecule are exploited for cryptographic purposes. The theoretical analysis shows this method to be efficient in computation, storage and transmission; and it is very powerful in certain attacks. On the other hand, in Mobile Ad Hoc Networks (MANETs): A Self Organizing and Adaptive Networks, has become one of the most prevalent area of research in the recent year because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location. But, Security solutions are important issues for MANET. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANETs are more prone to malicious attacks. This paper proposes scheme for handling data over untrusted network in air by using DNA Cryptography, which has become a corner stone in MANET security. In this paper, a proposal is given where the concept of DNA based digital encoding is being used in the encryption and decryption process. Unique cipher text generation procedures as well as a new key generation procedure for Wireless Mobile Network are proved to be powerful technique to provide high level of data security. This paper also proposes preventive measures against certain types of attacks that affect the MANET behavior due to any reason. Finally, to demonstrate the performance of the proposed method, its implementation is explained and the results are analyzed.***

Keywords: Mobile Ad hoc Network (MANET), DNA Based cryptography, Key generation, Encryption, Decryption.

1. Introduction

The security to a system is essential now a day! With the growth of the Information Technology and with the emergence of new techniques, the number of threats a user is supposed to deal with grew exponentially. It doesn't matter if we talk about bank accounts, social security numbers or a simple telephone call. It is important that the information is known only by the intended persons, usually the sender and the receiver. This is where the cryptography comes into picture. Cryptography is the basis of security of all the information.

Various cryptographic systems were developed in the past year. The recent development on this field is DNA Cryptography. This concept has emerged after the disclosure of computational ability of Deoxyribo Nucleic Acid (DNA). In this field of DNA Cryptography many research work is going on to make the computational process more complex to the unauthorized user. Well, presently it is in the development phase and requires a lot of work and research to reach an established stage.

The recent technology of data communication is an ad hoc mobile network also called as **M**obile **A**dhoc **NET**work (MANET). MANET is a collection of wireless mobile hosts that form a temporary network without the aid of any centralized administration or support (Figure 1). In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes interconnected by multihop communication path or radio links which are free to move at any speed in any direction and organize themselves randomly Figure-2. These wireless mobile nodes are constrained in power consumption, bandwidth, and computational power. MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks. Wireless links make MANETs more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is

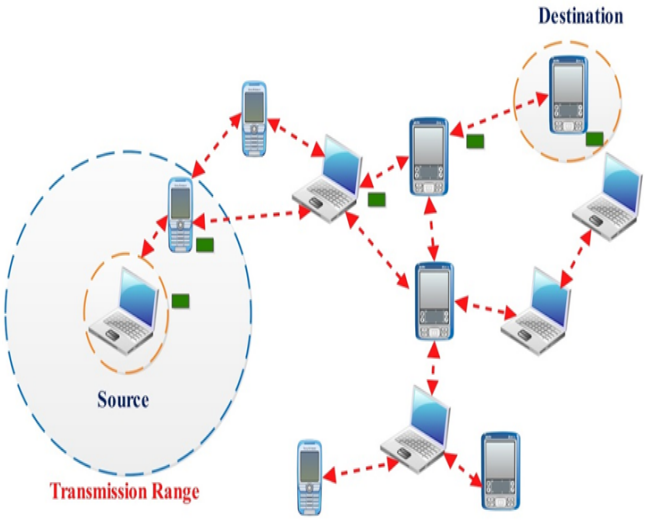

Figure 1: A Mobile Adhoc network

required. They can also directly attack the network to delete messages, inject false packets, or impersonate a node. This violates the network's goals of confidentiality, authentication, integrity, availability, access control, and non-repudiation Compromised nodes can also launch attacks from within a network. Ultimately, with those network Characteristics, security has become a primary concern for researchers to meet scientific challenges to market opportunities to achieve the above stated goals.

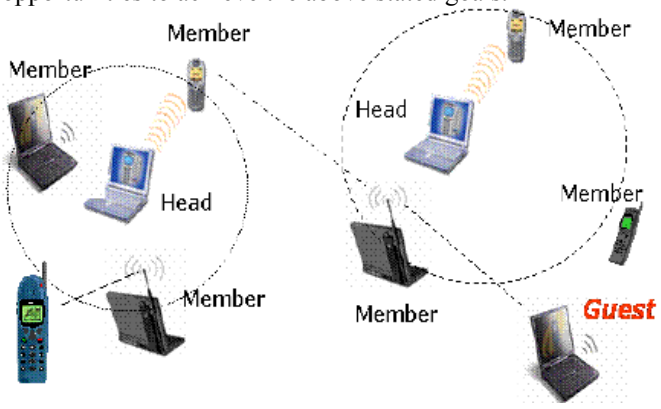

Figure 2: A Self-Organized Network [25]

On the other hand, DNA sequence based digital encoding tool is proved to achieve high data security. Thus, DNA based Cryptography can become a corner stone in MANET security by proposing an appropriate secure scheme for handling data throughout the network.

2. State of the Art

2.1 Network security in MANET

MANET security means the security mechanism for all protocols involved in this (MANET) service to protect the basic function of MANET means security during bit transfer from one node to another. Thus, MANET security involves authentication, key establishment and distribution, and encryption. Many researches are done on the security attacks and their prevention in MANET [13, 16].It is found that due to self-organizing nature of the network, there are lots of chances of security attacks at different layers of network architecture [13, 18-21]. Researches are still going on to prevent the network from various vulnerabilities. Routing protocols in [10, 11, 17] assume pre-existence and pre sharing of public and secret keys for all initial members. These protocols neglect key exchange and authentication, which are very important in MANETs. Recently Zhou and Haas [14] introduced the idea of distributing a CA throughout the network, in a threshold fashion, at the time of network formation. This CA would allow trust relations to be created in the network while also being resilient to some intrusions, malicious insiders, and breaks in connectivity. In [14], however, the resource limitations of devices in ad hoc networks are not addressed. Because public key and threshold cryptography are computationally expensive and require large memory, this method does not meet these resource limitations. Khalili, Katz, and Arbaugh [1] extended this technique to reduce the resources needed by using an ID–based system. Luo et al. [12] developed scalable, distributed authentication services in ad hoc networks. In their approach, multiple nodes collaboratively provide authentication services for any node in the network. Desmedt gives recent research aspects of threshold cryptography [24].Whereas, Mamatha has proposed the combine techniques from elliptic curve cryptography (ECC) and a distributed intrusion detection system (IDS) based on threshold cryptography, also proposed to use a distributed certifying authority (CA) along with per-packet per-hop authentication for addressing the issues like authentication, key distribution and intrusion detection [15].

2.2 DNA Based Cryptographic Technique

Secure communication can be achieved by employing strong cryptography to ensure confidentiality (nondisclosure of secret information), integrity (prevention of data alteration), authentication (proof of identity), and non-repudiation (unique, non-contestable message origin). These goals can be accomplished through a combination of symmetric-key algorithms (e.g. AES, DES, RC4), public-key algorithms (e.g. RSA, ECC), and cryptographic hash functions (e.g. MD5, SHA) [5] [23].

In the recent year few works on qualitative and quantitative analysis on DNA based Cryptography as well as many new Cryptographic techniques were proposed by the researchers [2-6] [20]. Bibhash Roy, et. al [5-9] proposed a DNA sequencing based encryption and decryption process. The authors propose a unique cipher text generation procedure as well as a new key generation procedure. But the experimental result shows that the encryption process requires high time complexity. This paper is enhanced from our previous proposed work [22]. This paper includes the procedures like public and private key generations; encryption and decryption for secure data communication using DNA based digital encoding technique in Mobile Adhoc Networks. This paper also shows the experimental result using Simulators and Emulators and proved to be far better technique as compared to other existing systems in terms of energy consumption, Time of execution, Data Security.

3. Proposed System

In actual scenario, DNA cryptography is far away from realization because in current time it can be performed only in labs using chemical operations. In order to provide better security and reliable data transmission an effective method of DNA based cryptography is proposed here. In this method the mixture of mathematical and biological concepts are used to get the encrypted data in the form DNA sequences. The benefit of this scheme is that it makes difficult to read and guess about data (plain text).The proposed algorithm has two phases in consequence: these are Primary Cipher text generation using substitution method followed by Final Cipher text generation using DNA digital coding

In the Primary Cipher text generation phase, the encryption algorithm uses OTP (one-time-pad) key generation scheme, since almost one key for one piece of information is sufficient to provide lots of strength in encoding technique. The proposed method uses randomly generated symmetric

key of 8 bits size by the intended receiver and provided to the sender. Thus the sender will have a partial knowledge of the private key only and then it generates the rest part of the keys (Private Keys: Level 1 and 2) to encode the information. The Byte values are extracted from the input file or message. The further encryption process works on unsigned byte values of the input file or text called as plain text. These byte values are replaced by combination of alphabets and special symbols using substitution method. And then this substitution values are converted into its binary value. In order to embed more security extra bits are padded at both the ends of the primary cipher text. These extra bits are nothing but the file size information, which is provided to the receiver through Level 2 key. Thus the secret key, the information of primer pairs are shared between sender and receiver through the secret channel.

In the DNA digital coding phase, the Final Cipher text is generated from Primary Cipher text using DNA digital encoding technique. From a computational point of view, we cannot process the DNA molecules as in form of alphabets, so the DNA sequence encoding is used in this method through which the binary data is converted into DNA format and it's vice versa. The four subunits of DNA molecule called as nucleotide bases: A: adenine; G: Guanine; C: Cytosine and T: Thymine are converted into 2 bit binary as A: 0(00), T: 1(01), C: 2(10), G: 3(11). Obviously, there are 4! =24 possible coding patterns by this encoding format. However, according to the Watson-Crick complementarily rule, in double helix DNA structure, the two DNA strands are held together complementary in terms of sequence, i.e. A to T and C to G. Taking DNA digital coding into account, it is required to reflect the biological characteristics of 4 nucleotides DNA bases, the complementary rule that (~0=1) and (~1=0) is proposed in [17]. As per the rules, 3(11) is complement of 0(00) and 2(10) of 1(01). So among 24 patterns, only 8 kinds of patterns (0123/CTAG, 0123/CATG, 0123/GTAC, 0123/GATC, 0123/TCGA, 0123/TGCA, 0123/ACGT AND 0123/AGCT) are fit as per complimentary rule of the nucleotide bases. It is suggested that the coding pattern 0123/CTAG is the best for nucleotide bases [17]. Thus A and T are corresponds to '00' and '11'respectively and C and G to '01' and '10' respectively. So substitution rule is A=00, T=11, C=01 and G=10 as illustrate in Table 1.

3.1 Algorithmic Presentation

The DNA based Cryptography algorithm using Secured Public and Private Key generation is as shown below:

Algorithm: DNA based Digital Encoding
Input: .txt; .doc; .jpg; etc. files.
Output: DNA based encoded file (.txt extension)

Begin
Step 1: Take the input file plaintext and convert into Byte code values.
Step 2: Use Substitution Method to convert pair of byte code values into the combination of special symbols and alphabets
Step 3: Generate two Primers i.e SPM(starting primer) and EPM(ending primer) from the input file size information.And perform sequence modification.
Step 4: Peform XOR operation with the primary key.
Step 5: Get the binary code of primary cipher.
Step 6: Use DNA digital encoding technique to convert this binary form of primary cipher into strong and complex DNA based cipher text.

End

Table 1: DNA digital Coding

Coding DNA nucleotide	Decimal	Binary
A	0	00
C	1	01
G	2	10
T	3	11

4. Result Analysis

We implemented this proposed method in java for its platform independent property. The proposed algorithm is applicable for almost all documents, image, text, pdf files. The graph represents the encryption and decryption time taken for certain file size. It is observed that the encrypted and decrypted file sizes are almost same (Figure 3.)

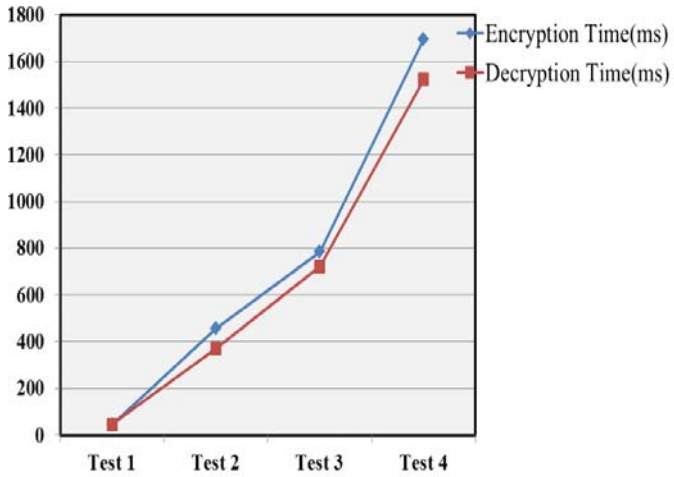

Figure 3: Encryption and Decryption Time Graph

4.1 Simulations and Emulation

An emulation platform allows you to understand the user experience for an application and test basic portability. For example, a platform enables you to run applications on several sample devices with different features, such as screen size, keyboard, runtime profile and other characteristics. Thus a flexible Java based Simulators and Emulators software called as Java™ Micro Edition Software Development Kit (version 3.0) is used to simulate network of windows mobile devices.

Java ME SDK provides three well-known emulation platforms: Connected Limited Device Configuration (CLDC) with MIDP, Connected Device Configuration (CDC) with AGUI, and CDC with Personal Basis Profile (PBP).All three platforms include predefined devices with different screen sizes, runtime profiles, and input methods.

The Table 2 shows the Simulators and Emulator that are used to show the real scenario of Mobile network. The

simulations allow maximum 9 nodes in the network and there should be no repetition of the simulator allowed. Always need to choose different simulators from the available menu driven mobile devices provided in the tool kit.

Table 2: Simulators and Emulators

Simulators Types	Emulator Platform
1. ClamshellCldcPhone1	CLDC Java(TM) Platform
2. DefaultCldcJtwiPhone1	Micro Edition SDK 3.0
3. DefaultCldcMsaPhone1	**Configuration of**
4. DefaultCldcPhone1	**Emulators**
5. DefaultFxPhone1	CLDC-1.1
6. DefaultFxTouchPhone1	**Device Profile:** MIDP-2.0

5. Resistance to Attack

In Mobile Adhoc Network, the typical attacks conclude malicious node attack, misbehave by a node attack. The scheme proposed in this paper can prevent these attacks.

A Malicious node attack: This attack is performed by a node which is unregistered. Thus such unauthorized nodes try to enter and disturb the network. The scheme we proposed can effectively prevent the attack of malicious node, because the attack nodes don't have the information of random key that is used to generate further private key for both data encryption and decryption. This is because, this random key information is provided with security between pair nodes and thus cannot be predicted by any other nodes in the network. So, such malicious nodes can't communicate with legal node within the network normally.

B Misbehave by a node attack: when the authorized node tries to read the message which is not for it, such attack is called as misbehave by a node attack. This proposed scheme can prevent from misbehave by a node attack because whenever any node who tries to read the data, its digital signature is verified in the network first. And, if the digital signature is verified and found correct, then it is allowed to read the data, otherwise not. So, if the legal node who tries to misbehave will not be able to read, since the data is encrypted in Digital DNA based strong encoding pattern.

6. Conclusion

The proposed method of encoding is far better and faster than conventional cryptography like DES and other DNA based encryption algorithm. DNA computing is a very promising field that keeps the ability to overcome many limitations of silicon computers. The Strength of the proposed method is the complex cipher generation from 8-bits keys. Although this method is efficient and powerful against certain attacks, the partial information contained in the cipher text makes the method much stronger. Also the digital DNA based encoding technique makes the cipher text ultimately very stronger than the existing systems do provide.

The proposed system is successfully designed and presented for MANET which satisfies the needs in mobile network. Typical attacks in wireless networks like misbehave and malicious nodes are prevented here. Our approach is scalable and flexible: variations and updates can be made in the node to node computation and design parameters can be adapted to fit the operational requirements of a particular Ad-Hoc network.

7. Future Scope

The proposal can be further enhanced to analyze its performance to other cryptanalytic attacks in mobile wireless networks and comparing it with existing security mechanism in MANET to know exactly how much improvement is achieved

Reference

[1] A. Khalili, J. Katz, and W. Arbaugh, "Toward Secure Key Distribution in Truly Ad-Hoc Networks," *in proceedings of the 2003 IEEE Symposium on Applications and the Internet Workshops*, 2013.
[2] Ashish Gehani, T. LaBean and J. Reif, "DNA-based cryptography", *IEEE transaction on DIMACS DNA Based Computers V, American Mathematical Society, 2000.*
[3] Ashish Gehani, Thomas H. LaBean and John H. Reif, "DNA-based Cryptography," *5th Annual DIMACS Meeting on DNA Based Computers(DNA 5)*, MIT, Cambridge, MA, June 1999.
[4] Ashish Gehani et al , "DNA-based cryptography", *Lecture Notes in Computer Science*, vol.2950, pp.167-188, 2004.
[5] Atul Kahate, "Computer and Network Security," *Tata McGraw-Hill Publication Company Limited*, Third Edition, 2013.
[6] Beenish Anam, Kazi Sakib,Md. Alamgir Hossain,Keshav Dahal, "Review on the Advancements of DNA Cryptography" *IEEE trans. arXiv:1010.0186v[cs.CR],* 1st Oct 2010.
[7] Bibhash Roy, Gautam Rakshit, Pratim Singha, Atanu Majumder, Debabrata Datta,"An improved Symmetric key cryptography with DNA Based strong cipher"-*IEEE trans. ICDeCom-2011*, Feb' 24-25'2011, pp.1-5.
[8] Bibhash Roy et al, "A DNA based Symmetric key Cryptography," *IEEE trans. ICSSA- 2011*, January 2011. p. 24-25.
[9] Bibhash Roy, Gautam Rakshit, Pratim Singha, Atanu Majumder, Debabrata Datta,"An Enhanced key Generation Scheme based cryptography with DNA Logic," *IEEE Transaction on IJICT-2010-11*, Volume 1 No. 8, December 2011.
[10] G.V.S. Raju, G. Hernandez, and Q. Zou, "Quality of service routing in adhoc networks," *IEEE WCNC 2000*, Vol. 1, 2000.
[11] G.V.S. Raju and G. Hernandez, "Routing in Ad hoc networks", *in proceedings of the IEEE–SMC International Conference.*
[12] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-Securing Ad Hoc Wireless Networks," *in proceedings of the 2002 IEEE Symposium on Computers and Communications*, Italy, July 2002.
[13] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and

Solutions," *IEEE Wireless Communications: 11(1),* February 2004. p. 38-47.
[14] L. Zhou and Z. Haas, "Securing Ad Hoc Networks", *IEEE Network Magazine, 13(6),* November/December 1999.
[15] Mamatha T., "Network Security for MANET", *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307*, Volume-2, Issue-2, May 2012.
[16] Muhammad Arshad Ali & Yasir Sarwar, "Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions," *School of Computing Blekinge Institute of Technology 371 79 Karlskrona, Sweden.* March 2011.
[17] P Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Networks," *IEEE trans. in proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference*, January 2002.
[18] Pradeep Rai, and Shubha Singh, "A Review of 'MANET's Security Aspects and Challenges," *International Journal of Computer Applications,* (0975–8887) Volume 9–No.12, November 2010.
[19] Priyanka Goyal et. al., "A Literature Review of Security Attack in Mobile Ad-hoc Networks", *International Journal of Computer Applications,* Volume 9–No.12, November 2010.
[20] Qinghai Gao, "A Few DNA-based Security Techniques", IEEE transaction Volume No. 978-1-4244-9877-2/11, 2011.
[21] Sevil Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks.pdf"
[22] Snehal Javheri, Rahul Kulkarni, "Secure Data Communication and Cryptography based on DNA based Message Encoding*," International Journal of Computer Application (0975-8887)*, Volume 98-No. 16, July 2014.
[23] William Stallings, "Cryptography and Network Security", *Prentice Hall International,* Third Edition, 2003.
[24] Y. Desmedt, "Some Recent Research Aspects of Threshold Cryptography," *in proceedings of the First IEEE International Workshop on Information Security*: 158–173, 1997.
[25] http://www3.ntu.edu.sg/ntrc/images/mobile2.gif

Author Profile

Snehal Javheri is a ME student, Department of Computer Engineering at Sinhgad Institute of Technology, Lonavala University of Pune. She has done BE in Computer Engg. Her area of interest is in Cryptography and Information Security, Mobile Adhoc Network Security and WSN Security.

Rahul Kulkarni has done BE (Information Technology) and ME (Software Systems). He is currently working as Assistant Professor at Sinhgad Institute of Technology, Lonavala University of Pune. His area of interest is in Network Security, Cryptography & information Security.