Evolving Fast Fourier Transform and Deoxyribonucleic Acid for security of RFID based authentication protocol

Vibhu[1], Harpreet K. Bajaj[2]

[1]*M.Tech Scholar CSE Deptt. DAVIET Jalandhar, Punjab, India* [1]
[2]*Associate Professor CSE Deptt. DAVIET, Punjab Technical University, India*[2]

Abstract - *RFID based applications used tagging and tracking of objects for tag and reader in IoT. RFID enables identification from distance, unlike earlier barcode technology. RFID system is vulnerable to various security threats and attacks. The aim of our paper is to make a hybrid technique by combining Fast Fourier Transform (FFT) and Deoxyribonucleic acid (DNA) sequence operations.Our proposed technique is different from existing technique in the sense that we are combining two encryption method techniques instead of concentrate on single technique. Our proposed hybrid technique is highly secure and it leads to performance gains when it compare to the existing technique experimentally.*

Key Words: RFID, Authentication protocol, Internet of things, FFT, DNA

1. INTRODUCTION

In a wireless network, during communication between two entities security is a major issue. While communicating, there is a secure connection between two entities when no third party interrupts communication and not even secretly listen the conversation. To protect this conversation between sender and receiver from being accessed by unauthorized users, cryptography method can be used. In cryptography, process of encryption occurs while scrambling of plain text into cipher text and then back again is decryption. The proposed hybrid FFT-DNA scheme is applied on RFID authentication protocol.

Radio Frequency Identification (RFID) is a wireless technology for the purposes of automatic identification of electronic tagsphysically attached to objects using an RFID reader [1]. Recently, RFID systems are widely employed in supply chain management, pharmacy management, library collection management, electronic payment systems, automatic toll collection, proximitycards, hospital patient care, containersearch within seaports and many more applications [2]. In general, RFID system composed of three main parts: tags, reader and backend server. A tag is a device which is physically attached to an object. Every tag has its own unique identification. Tags can be passive or active according to the power source [3]. Active tag has its inbuilt power supply, so it gets power from itself. While, reader produced electromagnetic field through which passive tag gets charged. A reader is a device that can recognize the presence of RFID tags and read the information supplied by them.

A server is a trusted entity. When the system is set up, all the information related to RFID tags identification is stored in server's database, through which mutual authentication is done. Using the stored identification information, the server could determine the validity of the tag. Usually, servers have high capability of computing as well as high memory capacity.

Recently, internet of things (IoT) is becoming as one of the most dominant communication model in the modern world. The basic idea of this concept is pervasive presence around us of a variety of things or objects such as Radio Frequency Identification (RFID) tags, sensors, actuators, and mobile phones etc. which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbours to reach common goals [4]. There are some application of IoT include: connected cars, smart city, home automation, wearable, smart grid, smart retail, industrial internet andtelehealth. In general, the DNA sequence are used to represent or encode the original data and the properties and DNA nucleotides are used a security enhancing feature which also helps to perform encryption and decryption of DNA sequence representing data.

On the other hand, Fast Fourier Transform (FFT) is a compression and encryption tool and applies to quite a few areas such as optical encryption and audio coding. To solve the problem of the low-level security and the great amount of data transmitted, FFT andDNA arecombined. The benefits of the proposed scheme are as follows: (1) The experiment suggest FFT and DNA method can resist man-in-the-middle attack, replay attack and impersonation attack. (2) Compared to ECC it can provide more security because of two-level security. (3) Receiver receives secure data with fast transmission speed.

The rest of the paper is organized as follows. Section 2 gives the related work. Section 3 discussed Existing ECC technique. Section 4 proposes FFT and DNA based authentication protocol. Experiments are discussed in

Section 5 followed by the results. Finally, this paper is concluded in Section 6.

2. RELATED WORK

Recently, RFID technology deployed in various applications especially as an identity management system, such as supply chain management, e-passports, and credit cards [2]. Currently, series of full-fledge RFID authentication protocol have been proposed. In 2012, Benssalah et al. [5] proposed an efficient challenge-response protocol based on elliptic curve EIGamal encryption schemes. They minimize the computation amount on the tag side by pseudo random number generation (PRNG), an elliptic curve point addition, and two scalar multiplications. They mentioned that their protocol resist from the following security attacks: passive attacks, man-in-the-middle attacks, replay attacks. Farash in 2014 [6], analyse Chou protocol and found that it suffers from lack of tag privacy, lack of forward privacy, lack of mutual authentication weaknesses. Also, it is defenceless to impersonation attacks, tag cloning attacks, and location tracking attacks. Then he proposes a more secure and efficient scheme to cover all the security flaws and weaknesses of Chous protocol.

Hannes et al. [7] presents an IPSec conform mutual authentication protocol with added attribute of privacy awareness for IoT infrastructure based on the Diffie-Hellman Integrated Encryption (DHIES) scheme [8]. It has been shown that the tag does not reveal the sensitive information unless it has assured that communication is initiated by the genuine backend reader which achieves privacy preservation concern of RFID carriers.

Zhang Leihong et al. [9] proposed FFT and CGI technique to solve the problem that large images can hardly be retrieved for stringent hardware restrictions and security level is low. This technique can be immediately applied to encryption and data storage with the advantages of high security, fast transmission and high quality of reconstructed information. In 2016, Xiuli Chai et al. [10] proposedan image encryptionalgorithm based on chaotic system and deoxyribonucleic acid (DNA) sequence operations. The plain image is encoded into a DNA matrix, and then a new wave-based permutation scheme is performed on it. Experimental results confirm that the proposed algorithm has not only an excellent encryption result but also resists various typical attacks.

3. EXISTING ECC TECHNIQUE

Various authentication protocols have been proposed to achieve certain security and privacy goals. Based on the RFID system resources, RFID authentication protocols can be classified into full-fledge class, simple, lightweight, ultra-lightweight authentication protocols. In the full-fledge class, the protocol requests the support of conventional cryptographic functions such as public key cryptography (PKC) or one-way cryptographic function. In fact, PKC assures highest level of security and privacy protection, but it is not fully supported by RFID system because of its high capacity requirement in term of key size and computational cost. One of the most attractive PKC solution is elliptic curve cryptography (ECC) as it provides the same level of security with smaller key sizes, faster computations, lower power consumptions as well as memory and bandwidth savings in contrast to the other PKC such as RSA. An elliptic curve is defined as a set of points (x,y) that satisfy an elliptic curve equation:

$E: y^2 = x^3 + ax + b$, where x, y, a and b are within a field. For cryptographic purpose those over the finite field of Fp and F2m are most suitable. The strength ofexisting protocol is based on two elliptic curve computational problem which are: elliptic curve discrete logarithm problem (ECDLP) and elliptic curve factorization problem (ECFP). ECDLP is to find $k \in [1, n - 1]$ such that $Q = k.P$where Q and P are two points over E. And the ECFP is to find the points $s.P$and$t.P$ from$Q = s.P + t.P$where$P, Q \in E$ and $s, t \in [1, n\text{-}1]$.

3.1 Algorithm:

Input : Sensor nodes, data (d)
Output : Secure data
STEP 1. Convert the communicating data into ASCII value
STEP 2. Apply ECC on data to generate random number
STEP 3. Deploy ECDH method for allowing public-private key pair for authentication
STEP 4. New changeable key encrypt the communication and decode data to ASCII value
STEP 5. Convert ASCII value to the secure data
STEP 6. End

3.2 Flow Chart:

The below flow chart elucidates, plain text is converted into its assigned ASCII value. ASCII value is generated to show the numeric value on elliptic curve, message is encrypted using private key and public key. Apply Elliptic Curve Diffie-Hellman (ECDH) method to calculate points on elliptic curve then these encrypted points are send to other site receiver. Now original message is retrieved by applying decryption process. In decryption, firstly decrypt points to original points using ECDH then it is converted to ASCII value and convert it into original text.

Table 1.DNA encoding rules

Rule	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

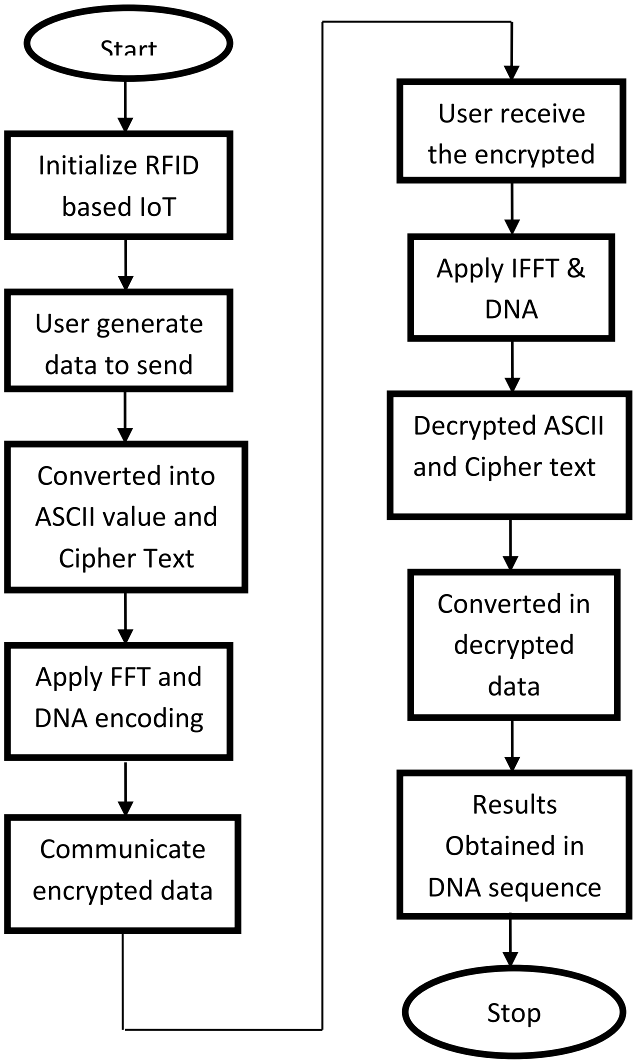
4.3 Algorithm:

Input : Sensor nodes, data (d)
Output : Secure data
STEP 1. Generate the data to send
STEP 2. Apply FFT and DNA on transformed data to convert it into encrypted form
STEP 3. Encrypted data to be communicated over the network
STEP 4. Apply IFFT and DNA decoding rule on encrypted data
STEP 5. Encrypted data then converted into decrypted form
STEP 6. Results obtained in DNA sequence
STEP 7. End

4.4 Flow Chart:

This flow chart elucidates the encryption and decryption process of RFID authentication protocol over a wireless network. Firstly, the RFID protocol will initialize then the user will request to IOT server which generate the data. The generated data will be in binary form. To make this communication secure, will apply fast fourier transform (FFT) on the transformed signal so that no hacker or cracker can crack the data. Then further apply DNA i.e. deoxyribonucleic acid on transformed signal to encode the FFT encrypted data. By applying, DNA our data will be more secured and completely in encrypted form.

After encryption, the process of decryption will start. Decryption will be done when the user receive an encrypted data. Inverse Fast Fourier Transform should be applied on the on encrypted data to decrypt it. Then further apply the DNA decoding rule to get the final result. Then end-user will receive the data and secure communication will be completed. Final result will be obtain in DNA sequence which will be in form of its four nucleotides i.e. A (adenine), C (cytosine), G (guanine), T (thymine). These are four acid bases of DNA which will provide the result and no hacker or cracker crack the encoding/decoding rules behind this. So in simple terms, this proposed protocol will be more secure and efficient than the existing one.


Start
Initialize RFID based IoT
User generate data to send
Converted into ASCII value and Cipher Text
Apply FFT and DNA encoding
Communicate encrypted data
User receive the encrypted
Apply IFFT & DNA
Decrypted ASCII and Cipher text
Converted in decrypted data
Results Obtained in DNA sequence
Stop

5. EXPERIMENTAL RESULTS

In this paper, FFT algorithm and DNA encoding rules are considered to obtain secure communication of RFID mutual authentication protocol. The simulation is conducted with the software of MATLAB. The software of MATLAB was used to simulate the development of RFID authentication protocol. The proposed hybrid protocol compared with ECC based RFID authentication protocol on the basis of different parameters: Storage, Overhead, Execution Time, Entropy and Bit Error Rate. These parameters shows that proposed protocol have better results as compared to ECC. Table 2 show that ensemble of FFT-DNA techniques delivers significant performance gains for almost all measures. However the performance of different parameters of both techniques may vary at different number of nodes.

We can take n number of nodes; here we have considered different nodes starting from Node 10 to Node 30. Then take the values of different parameters at different number of nodes. These values are shown in Table 2. From Table 2, we can see that as the number of nodes increases simultaneously, value of the parameters also increase it increase. Lower values derived as a result are better. These results have brought us to the conclusion that the overall performance of our protocol is better as compared to the existing derived results.

Table 2.Comparison proposed ensemble method (FFT-DNA) with ECC

Parameters	Number of Nodes									
	10		15		20		25		30	
	ECC	FFT-DNA	ECC	FFT-DNA	ECC	FFT-DNA	ECC	FFT-DNA	ECC	FFT-DNA
Storage	45.23	41.22	49.52	43.56	51.46	46.78	55.63	50.28	59.30	53.70
Execution Time	11.29	10.01	13.73	9.61	12.47	11.22	14.24	12.44	15.57	14.17
Entropy	1.73	1.25	1.84	1.41	1.76	1.31	1.81	1.09	1.60	1.44

5.1 Results

In this section, we discuss the results obtained using FFT-DNA technique for communicating data. These results are summarised as follows:

Storage: Storage refers to the process of placing newly acquired information into memory. ECC and FFT-DNA based values utilize the storage in memory. The lower is better. Fig 3 shows comparison from node 10 to node 30. The storage values are in kilobytes.

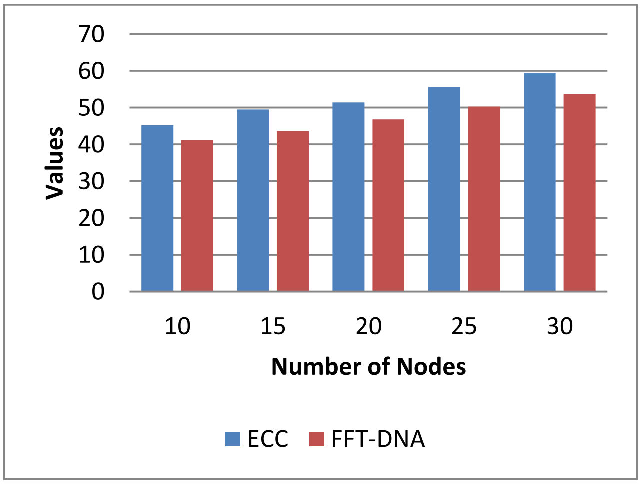


Chart – 1: Storage comparison of existing ECC and proposed technique FFT-DNA

Execution Time: Time taken to complete the task, it can be increase or more depending upon encryption algorithm. Fig 5 shows comparison from node 5 to node 21 for execution time. The time is calculated in seconds.

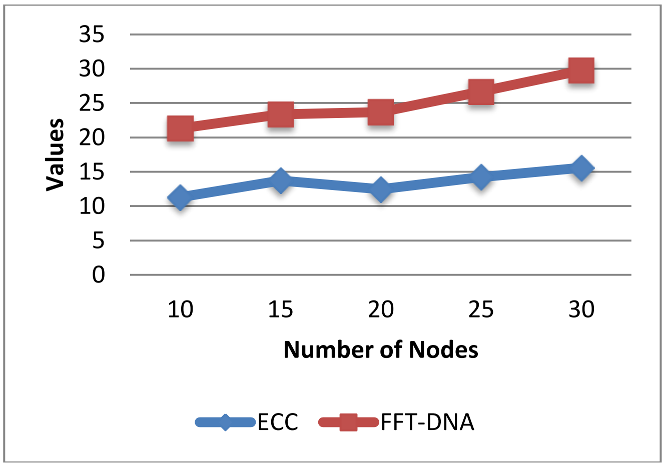


Chart – 2: Execution Time comparison of existing ECC and proposed technique FFT-DNA

Entropy - In computing entropy is randomness collected by an operating system for use in cryptography or other uses that require random data. A lack of entropy can have negative impact on performance and security. Entropy is measured in Hart (Hartley).

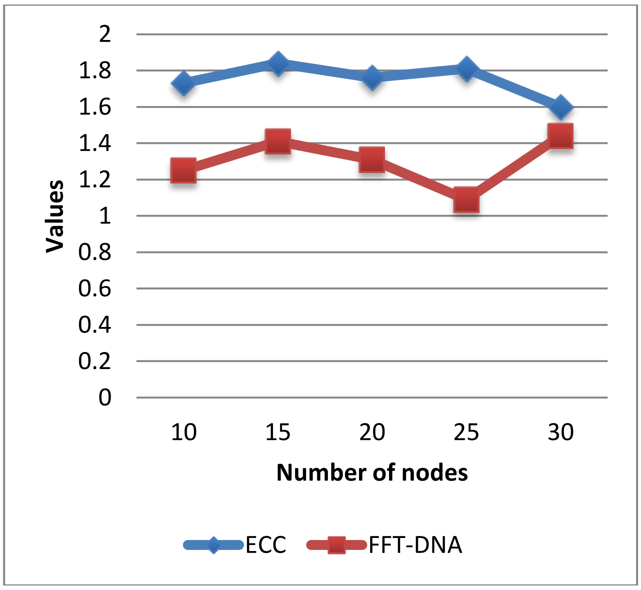


Chart – 3: Entropy comparison of existing ECC and proposed technique FFT-DNA

6. CONCLUSION

In this paper, the feasibility and security of FFT-DNA method were verified. According to experiment it can be concluded that, our proposed FFT-DNA based authentication protocol eliminate the current RFID vulnerabilities raised be insecure channel between tag and reader. A random number generated during the process and its ASCII code is converted into cipher text i.e. encrypted message. Further, it converted into decrypted ASCII message and at last user receives encrypted message. Our experimental results have better and efficient solutions as compared to the existing technique. And with this, new results derived are far better than the earlier technique. These two techniques are compared with each other by considering the three parameters including storage, execution time and entropy. All these features show that our technique has a high security level and is very suitable for encryption.

References

[1] Roy want. “An introduction to RFID technology.” IEEE pervasivecomputing 5.1 (2006): 25-33.

[2] Stephen B. Miles, et al. “RFID technology and applications.” Vol.1 Cambridge: Cambridge University Press, (2008).

[3] Amjad Ali Alamr. “A secure ECC based RFID mutual authentication protocol for Internet of Things.” Springer New York, (2016).

[4] Luigi Atzori, et al. “The Internet Of Things: A Survey” Computer Networks (2010).

[5] Mustapha Benssalah, et al. “RFID authentication protocols based on ECC encryption schemes.” IEEE international conference on RFID-technologies and applications, RFID-TA 2012, Nice, France, November 5-7 (2012), pages 97-100.

[6] Fararsh Mohammad Sabzinejad, et al. “Cryptanalysis and improvement of a robust smart card secured authentication scheme on SIP using elliptic curve cryptography.” Multimed Tools Appl 75(8) (2016): 4485-4504.

[7] GrossH, Slamanig D, et al. “Privacy-aware authentication in the internet of things.” Cryptology ePrint Archive, Report (2015)/1110.

[8] Michel Abdalla, et al. “The oracle diffie-hellman assumptions and an analysis of dhies.” In: Naccache D (ed) CT-RSA, volume 2020 of lecture notes in computer science. Springer, Berlin, (2001), pp 143-158.

[9] Zhang Leihong, et al. “High-performance compression and double cryptography based on compressive ghost imaging with the fast fourier transform.” Optics and Lasers in Engineering 86 (2016) 329-337.

[10] Xiuli Chai, et al. “A novel chaos-based image encryption algorithm using DNA sequence operations.” Optics and Lasers in engineering 88 (2017) 197-213.

[11] Hoda Jannati, et al. “Cryptanalysis and enhancement of a secure group ownership transfer protocol for RFID tags.” Global Security, Safety and Sustainability & e-Democracy. Springer Berlin Heidelberg, (2012): 186-193.

[12] Zahra Ahmadian, et al. “Desynchronization attack on RAPP ultralightweight authentication protocol.” Information processing letters 113.7 (2013): 205-209.

[13] Chiu C. Tan, et al. “Secure and serverless RFID authentication and search protocols.” IEEE Transactions on Wireless Communications 7.4 (2008): 1400-1407.

[14] Yanjun Zuo. “Secure and private search protocols for RFID systems.” Information Systems Frontiers 12.5 (2010): 507-519.

[15] Yong Ki Lee, et al. “Low-cost untraceable authentication protocols for RFID.” Proceedings of the third ACM conference on Wireless network security. ACM, (2010).

[16] Md.Endadul Hoque, et al. “Enhancing privacy and security of RFID system with serverless authentication

and search protocols in pervasive environments." Wireless personal communications 55.1 (2010): 65-79.

[17] Mari Carmen Damingo. "An overview of Internet of Things people with disabilities." Journal of Network and Computer Applications 35 (2012) 584-596.

[18] LaiphrakpamDolendro Singh, et al. "Implementation of text encryption using Elliptic curve cryptography." Procedia Computer Science 54 (2015) 73–82.

[19] Debiao He, et al. "An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography." IEEE Internet of Things Journal, Vol.2, No.1, (2015).

[20]Jue-Sam Chou."An efficient mutual authentication RFID scheme based on elliptic curve cryptography."JSupercomput (2014) 70:75-94.

[21] MasoumehSafkhani, et al. "On the security of Tan et al. serverless RFID authentication and search protocols." International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer Berlin Heidelberg, (2012).

[22] Wang Yujing, et al. "An image encryption scheme using mixed high dimensional chaotic system combined with fast fourier transform." IEEE 12th International conference on electronic and measurement & instruments (2015).

[23] HangRok Lee, et al. "The tag authentication scheme using self-shrinking generator on RFID system." Transactions on Engineering, Computing, and Technology 18 (2006): 52-57.

[24] Qiang Zhang, et al. "Image encryption using DNA addition combining with chaotic maps." Mathematical and Computer modelling 52 (2010) 2028 – 2035.

[25] Qiang Zhang, et al. "A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system." Optik 124 (2013) 3596 – 3600.