ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Random Frequency Transmission (RFT): A Confidential Data Transmission Approach

Dipesh Vaya
M.Tech. Scholar, Department of Computer Science and Engineering Geetanjali Institute of Technical Studies Udaipur, India
dipesh.vaya88@gmail.com

Devanshu Paliwal
M.Tech. Scholar, Department of Computer Science and Engineering Geetanjali Institute of Technical Studies Udaipur, India
devpal24@rediffmail.com

Sarika Khandelwal
Assoc. Prof., Department of Computer Science and Engineering
Geetanjali Institute of Technical Studies Udaipur, India
sarikakhandelwal@gmail.com

Abstract: In the present era of digital communication where we have various data transmission techniques are generally relies on cryptography for security. But when we are concerning with data related to international/national security, we have to ensure more powerful security mechanisms. As technology is enhancing day by day enemies/intruders are also growing as well. In this paper we will discuss some parameters of Random Frequency Transmission (RFT) in private military area i.e. the data can be secured by sending it on different frequencies.

Keywords: Cryptography, Frequency Distribution, Cryptography Algorithm, Factoralization, Quantum Cryptography.

I. INTRODAUCTION

Cryptography is the fundamental operation in information and data security [1]. It is useful in a number of tasks such as information secrecy, secured communication, and data compression cum encryption. As many cryptographic algorithms have been incorporated to make the communication secure but the intruders are also trying to make themselves a bit ahead.

The problem of information hacking is more critical when the information is related to national security. In modern scenario the communication between two military head quarters is done in a much secured way but still we are worry a bit about present security mechanism. In a cryptographic communication system we encrypt the information by encryption algorithm using a symmetric or asymmetric key [1,2] and then we send it the intended receiver using a medium which can be either a physical (if the communication is in within the office or building) or wireless (if the communication area is wider such as using internet). But the real problem arises from here as the enemy or intruder tries to hack the particular information transmitted between two communicating parties. If the intruder does not have any idea about the encryption algorithm and the key used while encryption operation then it is very much difficult to hack the information but we cannot say it is impossible.

An intruder can be able to predict the security mechanism used after a deep analysis of information transferred between two parties and if intruder's prediction becomes his success then it will be very disastrous to a particular nation. So this problem is very crucial and it should be resolved.

In general an intruder can attack on our communication & security system from below given possible points (i) either he/she can hack the sender's system (ii) or he/she similarly can hack the receiver's system (iii) or either the information can be hacked from the point where it is being travelling from sender to receiver while information transmission. Points (i) and (ii) are very impractical in present security mechanism techniques as an intruder must have physical accesses to the sender's and receiver's computer systems, which is not easy or we can say impossible.

So the only way intruder can attack is while the information is travelling in the medium. So if we can be able to make our information transmission process highly reliable and secure then there is a less chance to be a victim of security attack. In present security system a lot of practice is done on cryptography to secure the data as we believe that the intruders will be able to attack on the communication system and they will retrieve all the encrypted information by hacking encryption or decryption key.

As we know that active attacks are easy to detect and we can easily prepare to cope with but passive attacks are not easily detectable. In passive attack there is no way to find out that we are the victim of such security attacks or not. Random Frequency Transmission (RFT) is designed to save us from passive kind of attacks.

CONFERENCE PAPER
II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council , IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

This paper is organized as follows. A brief review of the Random Frequency Transmission (RFT) techniques. After Next section data transmission process and related issues are illustrated. Finally, we concluded our work.

II. THE OBJECTIVE FUNCTIONING OF RFT

The transmission approach can be serial or parallel. Present scenario tends to focus on the use of serial transmission of fragments because of the relative ease in maintaining the stability of the system. In the process of Random Frequency Transmission (RFT) there are two communicating machines or computer systems one of which is acting as sender and another as receiver.

An application software which generates random frequency number in between the given range will be installed at both communicating machines. The application software generates a random frequency each and every time when required using a global key value (a global key value can be any value that is global for both the communicating machines).

The benefit of using a global key value is that it will turn our application software to generate a random frequency in synchronization i.e. the frequency generated at sender's machine will be as same as generated on receiver's machine at any instance of time. The sender transmits the information on the frequency that is generated (at both machines) by application software as same frequency is also generated at receiver side it will starts to receive the data on the same frequency after some delay. And for acknowledgement of successful communication we can incorporate handshaking protocol [5]. So only the sender and receiver are aware about the frequencies on which communication will be done. Detailed process is described in the following sections.

III. PROCESS AT SENDER'S - END

A. Information Processing:

This is the first operation which is performed in the process of Random Frequency Transmission (RFT). In this phase information is prepared for transmission process. In preparation phase the information or message is divided into two or more fragments. The size of fragments can be arbitrary. After that each fragment is assigned a unique id number in sequence using a unique id generator program. For an example if a message is of 24 kb and we decided to break it in 4 fragments and these fragments can be any arbitrary size. Some possible fragments can be as depicted below in figure 1.

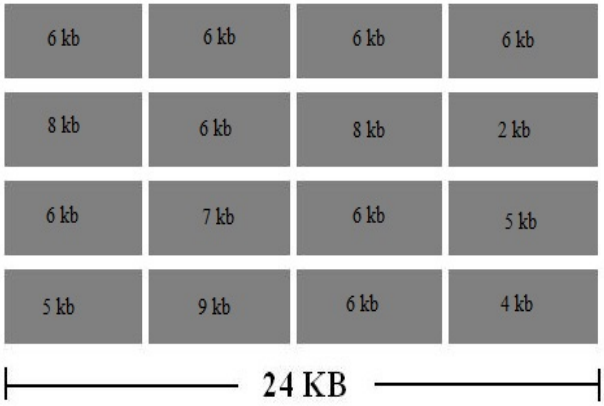

Figure 1. The possible 4 ways to break the information of size 24 kb into 4 fragments of arbitrary size

Let we choose the fragments of size 8 kb, 6 kb, 8 kb, 2 kb. And now we will assign an arbitrary unique id number to each fragment in sequence. The first letter of unique id will contain the number of fragments that are to be transmitted. In our example let we generated a 5 digit unique id then the unique id will start from digit 4 as there are 4 fragments.

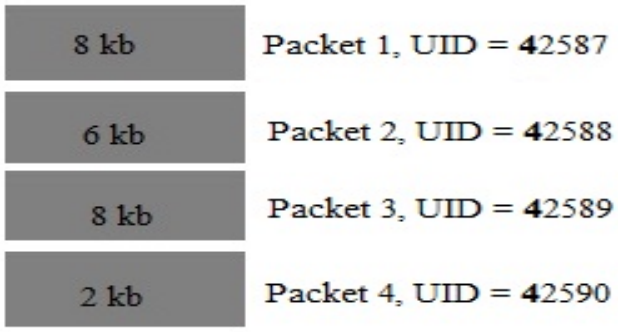

Figure 2. Unique IDs generated for each fragment by unique id generator

As described previously here in all unique id's the first digit is same (here it is 4) and is equal to the number of fragments. Remaining last four digits describe the proper sequence of the fragments (for the given example these are **42587**, **42588**, **42589**, **42590**). This unique id is then attached with each fragment to be transmitted.

B. Information Security:

This is the next phase after information processing section. In this phase we will perform some encryption operations to make information secure. Each fragment (including unique id) is taken and encrypted with an encryption algorithm. For encryption we can incorporate any encryption algorithm like DES, and RSA. As DES was cracked many years before and RSA was more powerful than DES. The RSA algorithm becomes very popular from the last couple of years. But unfortunately RSA algorithms can be cracked by P. Shor's high-speed quantum algorithms in quantum computing using factoralization [4,7].

So a new approach was required to make information more secure an after some of researches a new encryption

CONFERENCE PAPER
II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

technology is discovered which is known as Quantum Cryptography [3]. Quantum cryptography provides inclusive security as it is based on elementary physical laws. In Quantum Cryptography technique the key distribution is done in sophisticated way using fibre optics cable. But Quantum Cryptography technique is optimum when two communicating devices are at lower distance. But if two communicating devices are situated at a very long distended geographical area then we have to set up a fibre optic cable to connect them with each other which is not possible practically and if anyhow we managed to setup such huge network of fibre cables then also we will not be able to solve the problem due to the slower transmission speed (key distribution speed) i.e. 1.1 kbps, and the error rate of 1.7% over the transmission distance of 200m [4].

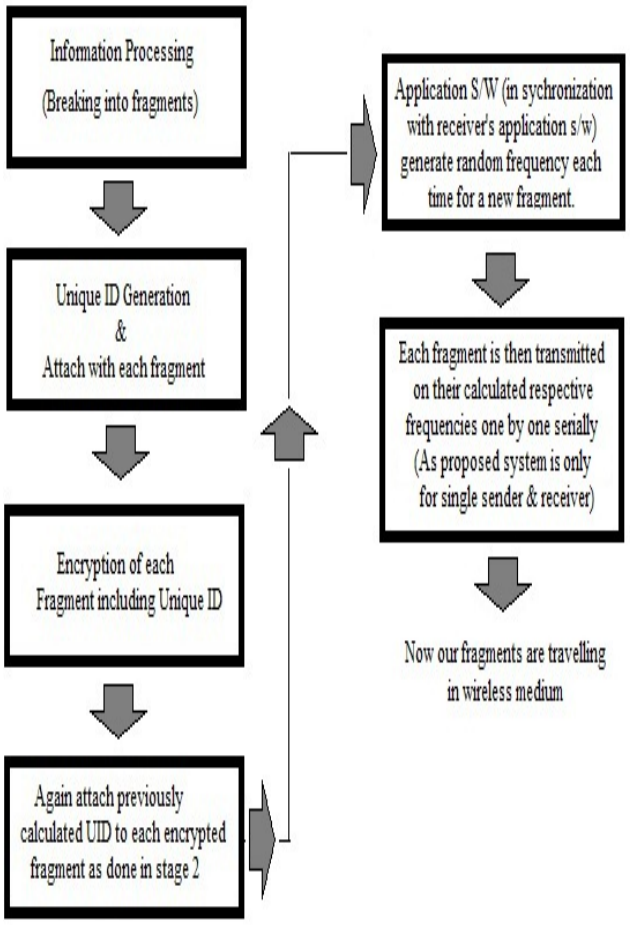

Figure 3. Operations performed at sender's side

Quantum Cryptography technique is best approach when communicating devices are at nearer geographical positions. To solve this problem we can use another cryptography technique which is known as Cryptography using Genetic Algorithms [6,8]. In this approach we make use of some genetic algorithms to encrypt the data.
After encryption previously calculated unique id is again attached with each fragment to be transmitted. Now these fragments are ready to transmit.

C. Transmission Process:

While transmission of the fragments the application software at sender's machine generates a random frequency number at the same time application software at receiver's side also generates the same random frequency number as both application software uses a global key to generate the random frequency number. Fragments are transmitted one by one in serial and for each new fragment a new random frequency is generated in synchronization.
For example for the first packet having UID = 4**2587** and of 8 kb in size the application software will generate a random frequency number let it is 228.9 Hz. And this packet is transmitted on this frequency the receiver also knows that a packet is coming towards it on frequency 228.9 Hz. due to application software. Similarly the second packet having UID = 4**2588** and of 6 kb in size the application software will again generate a random frequency number let now it is 382.2 Hz. And the same procedure is repeated for each and every packet or fragment.

IV. PROCESS AT RECEIVER'S – END

The receiver receives all fragments one by one from their respective frequencies generated by application software. Simultaneously on reception of each fragment the Unique IDs are de-attached from each fragment one by one. And then decryption algorithm is applied to the encrypted fragments (excluding UID attached at stage 4 while sending.). After decryption we will get the first original part of message and a UID which was attached previously to the fragment in stage 2 while sending. Again we de-attach this UID from original message.
Now we will perform a comparison operation which will compare both UID's. If two UID's are not equal then immediately receiver will send a warning or error message to sender in order to stop the further transmission of fragments.
If both UID's are equal then we can say that our message is not attacked by any active attacker. Then first bit of UID is checked to know the number of fragments being transmitted by the sender.
After receiving all the fragments the receiver machine will send an acknowledgement message denoting the successful reception of all fragments according to handshaking protocol.
In the case if acknowledgement message is not received by the sender then all the fragments can be transmitted again to the receiver.
And if receiver sends a warning or error message after comparison of both UID's (the one i.e. de-attached in stage 2 and another i.e. de-attached after decryption in stage 4 at receiver's end.) , which are not equal, then receiver will discard all the fragments received and sender will immediately stop the sending of further fragments. And then entire process will be repeated from start to retransmit the message fragments.

CONFERENCE PAPER
II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

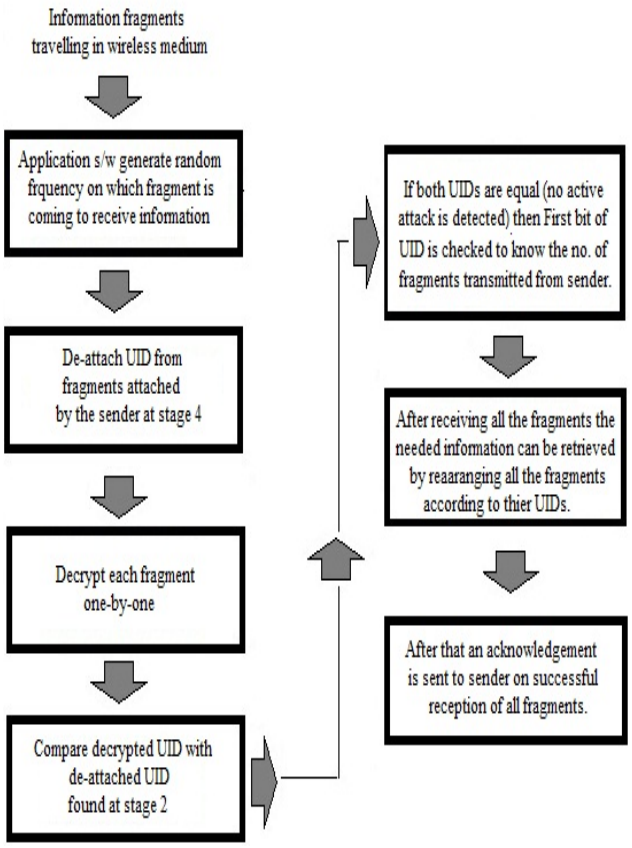

Figure 4. Operations performed at receiver's side

The whole process & operations performed at receiver's side after receiving the information are depicted above in figure 4. So in this way the Random Frequency Transmission (RFT) technique enhances the security of information using random frequencies.

V. CONCLUSION

We have introduced the Random Frequency Transmission (RFT) approach for confidential data transmission. This approach incorporates the encryption of information & then transmission on random frequencies. For military purpose this approach can be useful to send and receive very confidential messages, mails, and information of small size. This approach seems to be very attractive and safe with respect to presently available approaches because it is very random in nature therefore very difficult to judge. So our proposed Random Frequency Transmission (RFT) approach will protect our confidential information against any kind of passive security attack as well as active kind of security attack.

VI. REFERENCES

[1] Michael E. Whitman, Herbert J. Mattord, "Principles of Information Security", 4/e, Cengage Learning, 2012.
[2] William Stallings., "Cryptography And Network Security : Principle And Practice", 2/e, Prentice Hall,1999.
[3] Nishioka, T., et al: Circular Type Quantum Key Distribution, IEEE Photonic Technology Letters vol.14, No.4 (2002).
[4] Toshio Hasegawa and Tsuyoshi Nishioka (2002), Technical Reports on Quantum Cryptography: Mitsubishi Electric Corporate News Release, vol. December, 2012, pp. 18-22.
[5] Douglas E Comer, "Hands-on Networking with Internet Applications",2/e, Addison-Wesley, 2004.
[6] Ankita Agarawal, "Secret Key Encryption Algorithm Using Genetic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, April 2012, pp. 216-218.
[7] Samuel J. Lomonaco, Jr., "A Quick Glance at Quantum Cryptography", quant-ph/9811056, Nov. 23,1998.
[8] A. J. Bagnall, "The Applications of Genetic Algorithms in Cryptanalysis", School of Information System, University of East Anglia, 1996.