International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 7, July 2013 ISSN 2319 - 4847

Efficient Cryptography with Compression/Decompression Mechanism of Text Files against IP spoofing

Rupinder Singh Brar[1], Sarpreet Singh[2]

[1]*Student of masters of technology Computer Science,*
Department of Computer Science and Engineering,
Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India.

[2]*Assistant Professor, Department of Computer Science and Engineering,*
Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India.

ABSTRACT

Internet becomes a backbone of every sector, which gives essential information of each domain like education, concerns, entertainment etc. Data stealing and data theft is the well known thing in networks. IP spoofing is one of the techniques of data stealing in the form of malicious IP address. Spoofed packet can steal our data or may reduce bandwidth size and resource utilization etc. In this paper we provide an efficient method to prevent from the IP spoofing using two way security mechanism compression and encryption and compared the Result with Previous Results which is more efficient in terms of time and network bandwidth utilization.

Keywords: IP spoofing, Compression, Bit reduction algorithm, Cryptography, NTRU mechanism.

1. INTRODUCTION

1.1 IP spoofing [5]

IP Spoofing is one of the major tools used by hackers in the internet to mount denial of service attacks. In such attacks the attackers duplicate the source IP of packets that are used in the attack. Instead of carrying the original source IP of the machine the packet came from, it contains an arbitrary IP address which is selected either random fashion or particularly. The ease with which such attacks are generated made them very popular. There are at least four thousand such attacks happening every week in the Internet. In a spoofing attack, the intruder sends messages to a computer indicating that the message has come from a trusted system. To be successful, the intruder must first determine the IP address of a trusted system, and then modify the packet headers to that it appears that the packets are coming from the trusted system.

1.2 Compression[5]

Basically compression classified into two types-

1.2.1 Lossy Compression

In Computer terminology, lossy compression is a data encryption method which eliminates some of the data, in order to achieve its goal, with the result that decompressing the data yields content that is different from the original, though similar enough to be useful in some way. Lossy compression is most commonly used to compress multimedia data, audio, video, image, etc. lossless compression is required for text and data files, such as bank records, text articles, etc. In many cases it is advantageous to make a master lossless file which can then be used to produce compressed files for different purposes.
We can compress many formats of digital data through that we can minimize the size of a computer file needed to store it. According to the networks the effective utilization of bandwidth needed to stream it, with no loss of the full information contained in the original file.

1.2.2 Lossless Compression

Lossless data compression is a kind of data compression algorithms that allows the exact original data to be fetched from the compressed ZIP data. The term lossless is in contrast to lossy data compression, which only allows an approximation of the original data to be re fetched, in exchange for better compression rates. Lossless data compression is used in many applications.

1.3 Cryptography [6]

Cryptography has been used as a way to send secret messages between warring nations, between users, between organizations etc; as such, it became an important issue in national security and laws. With the increasing need for secure transactions for data traversing computer networks for medical, financial, and other critical applications, cryptography is now becoming a necessity for nongovernmental, nonmilitary applications.
Cryptography has some major issues:
Key length: The combination of the algorithm and the key length are factors of cryptographic strength. The algorithm is usually well known. The longer key is the stronger the cryptographic strength of a given algorithm. Some countries have export laws that limit the key length of a given cryptographic algorithm.
Key recovery: In recent years, export laws have been modified if the cryptographic algorithm includes the capability of incorporating key recovery methods. These modified laws enable governments to wire-tap for encrypted electronic data if they deem it necessary to do so.
Cryptography use: A distinction is sometimes made about whether cryptography is used for authentication and integrity purposes or for confidentiality purposes. When used for confidentiality, the export laws are typically much more stringent.
In this paper cryptography uses to enhance the security in IP compression technique as well as the Mechanism that one is used is more efficient than previous one. It takes too less time to encrypt the file with Cryptography Mechanism.

2. RELATED WORK

In the Previous research GRS compression was implemented with RSA mechanism for cryptographic use for protection of data from unauthorized access. But we have one limitation of RSA mechanism as it takes too much time to encrypt the File. So we have implemented NTRU Mechanism which is more secure, Fast and Robust than RSA.

3. PROPOSED METHOD

We have incorporated NTRU encryption mechanism to provide the Security of our data from unauthorized users and with the advantage of fast mechanism to encrypt the File. This Mechanism is more secure, robust and fast than RSA mechanism. So we have tried to implement this mechanism with compression to achieve better results from previous Research.

3.1 Methodology

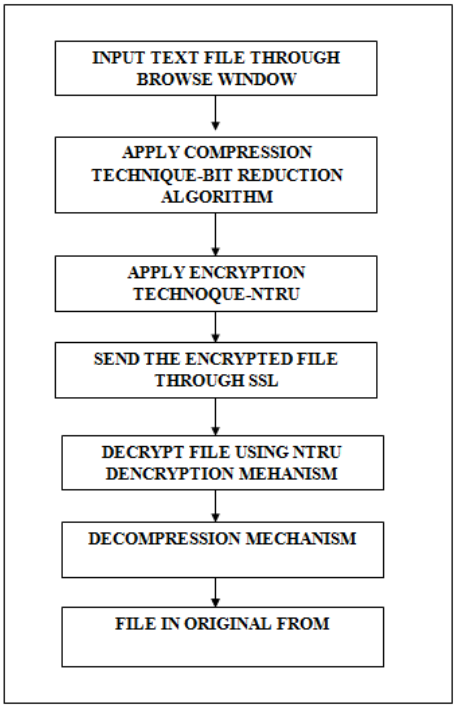

Figure1 Methodology of Research work

3.2 Input Text File Through Browse Window

At First we will browse our window and pick up the text file which would we placed in c drive and load it in our database where we compress and encrypt it through two different mechanism in a single way.

3.3 Apply Compression Technique-Bit Reduction Algorithm

Then we apply the basic compression algorithm which would reduced the file size upto its 25%to 40%.so that we can utilize our network bandwidth properly.

3.3.1 Implementation of Bit Reduction Algorithm as-

- Main Idea of algorithm—This reduces the standard 8-bit encoding to some application specific 6-bit encoding system and then pack into a byte array. This method will reduce the size of a string considerably when the string is lengthy and the compression ratio is not affected by the content of the string.
- A constant for flag the operation as 6-bit conversion.
- This algorithm is demonstrating the use of class SixBitEnDec using a simple interface. You can insert some texts and observe the size of the text after compressing and also the text after decompressing.

3.3.2 Steps To be followed in this algorithm- Compression

a) 6 bit algorithm based on binary number system.

Code table is build up for assignment of numeric values to different character set.

b) Assumption-

1. Assign the numeric value 0 & 1 to ‘ ‘ and .
2. Assign the numeric values from 2 -26 to Small letters i.e a-z.
3. Assign the numeric values from 26-53 to capital letters i.e A-Z.
4. Assign the numeric values from 54-63 to numeric's i.e 0-9

c) Now pick up the text file and characters inside them.

d) Now obtain binary code of each character set of text file as along the assumption in code table.

e) Now chop off two distinct places from binary number obtained from code table.

f) 1 byte=8 bit after chop of two distinct it will be of 6bit per each character.

g) Now collect each reduced bit into single array

h) Fill will be compressed.

3.4 Apply Encryption Technique-NTRU

NTRU cryptosystem is a relatively new public key cryptographic algorithm that was first introduced in 1996. The main advantage of this algorithm is that it runs much faster than conventional public key algorithms such as RSA. This speed advantage is especially large in key generation, which is often the most important part of public key cryptography. NTRU is the first public key cryptosystem not based on factorization or discrete logarithmic problems. NTRU is a lattice-based alternative to RSA and ECC and is based on the shortest vector problem in a lattice.

3.4.1 Implementation of NTRU Algorithm

NTRU KEY AND PARAMETERS

n-The Polynomial in the Ring R have Degree N-1(Non-Secret)
p-Large modulus Prime number in Which each coefficient is reduced.(Non Secret)
q-Small Modulus Prime number in which each coefficient is reduced.(Non Secret)
d- Polynomial in private key.
e- Prime number to generate Public key.
Ø-A function which is the combination of Large modulus value and small modulus value after reduction.
Encryption Key-Public key—(n, e)
Decryption Key-Private Key-(n ,d)
KEY GENERATION –Public key For Encryption- Encryption Key-Public key—(n, e)

a) User A Randomly Chooses Two Prime No. P and Q Such that P≠Q and Generate n that would be multiply of P and Q.

n=pq and Ø=(p-1)(q-1)

b) e should be prime number such that Greatest common Factor (gcd) of **(e, Ø)=1.**

c) Encrypt the Message M with the following Equation

E(M)=(M)^e mod n

Encrypted Message will be created with Public Key.

3.5 Send the Encrypted File through Secure Socket Layer

After compress and encrypt the file through different mechanism in the single way then we will send this file which is in form of cipher text through the secure socket layer. After sending the file from the server end, we will receive it at client end where we decrypt, it as well as decompress it and finally get it in original form.

3.6 Decryption Mechanism

KEY GENERATION –Private key For Decryption- Decryption Key-Private Key-(n ,d)

a) Follow the steps (i),(ii),(iii) In Encryption for the value of **e** and **Ø** such that it satisfy the mathematical Notation:

e.d = 1 mod Ø--------(1)

b) After Rearranging the Equation 1 **Using Extended Euclidean Algorithm** for our own convince we have equation as:

e.d + Øk= 1 s.t k is constant value.---(2)

c) Now to find the value of d and k

suppose d=x and k=y insert them in equation (2).

Equation becomes :

ex+ Øy=1

Then Randomly find the value of x and y which satisfy this equation and then reassign the value of x to d.

d) Using Equation:

D(E(M))=(E(M))^d mod n.

then it would be value of Decryption Message.

3.7 Decompression Mechanism

Decompression Mechanism at the client side is followed in following steps:

a) Receive compressed file at client side.

b) Add on 256 binary no to each bit in in byte array.

c) Then divide the byte array with multiple of 8 (1 byte=8bit)

d) Now obtain the character from each binary number obtain after division of multiple of 8.

e) File will be decompressed/decoded in original text in D drive where its path is specified

3.8 File in Original Form

After whole working, we will receive file in the original size as well as original format at D drive which is specified path for the decrypted and decoded file.

4. RESULTS AND COMPARISON

The Research is carried on different size of text files with purposed algorithm which include compression with Bit-Reduction algorithm and cryptography with NTRU and significant results are obtained as compared to the previous Research which was based on GRS compression algorithm with RSA cryptography.

4.1 Comparison

The Results are compared in terms of time taken to complete mechanism, which include compression, Encryption, Decryption and decompression. The algorithm which is purposed is tested on java platform with Net beans software and results are obtained with Microsoft excel sheet.

4.2 Performance Parameters

The comparison of two algorithms is done on the basis of following performance parameters:

4.2.1 Encryption Time: Files will be encoded and encrypted with NTRU mechanism and we have taken the result set of four files based on Encryption time for each file and build up a table and compare the encryption time for previous result set which include RSA and GRS encryption time and Results are presented on the Graph.

4.2.2 Decryption Time: The Same Files the decoded and Decrypted at client end with the same mechanism of Bit-Reduction decompression cum NTRU decryption and Results are recorded on same set of four files and compare with the Previous results. The Results are Quiet significant than last one and presented on the Graph.

4.2.3 Overall Time Taken: At last the the overall time taken by both the algorithms are compared and Presented. The overall time taken includes the Encryption, Compression, Decryption and decompression time. We find that our Purposed algorithm is Quiet Efficient than the previous one in terms of time taken to carry out the whole mechanism as well as compression ratio.

4.3 Comparison using Encryption Time:

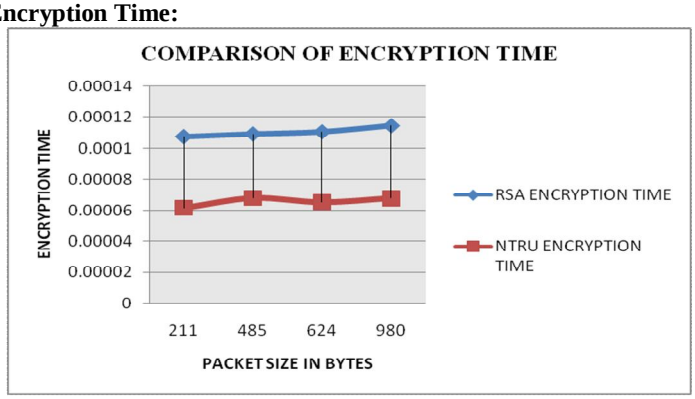

Figure2 Comparison using Encryption Time

4.4 Comparison Using Decryption Time:

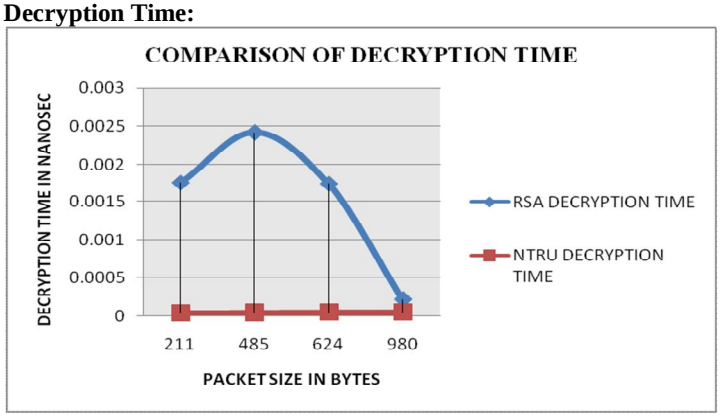

Figure 2 Comparison Using Decryption Time

4.5 Overall Time Comparison with Both Mechanisms:

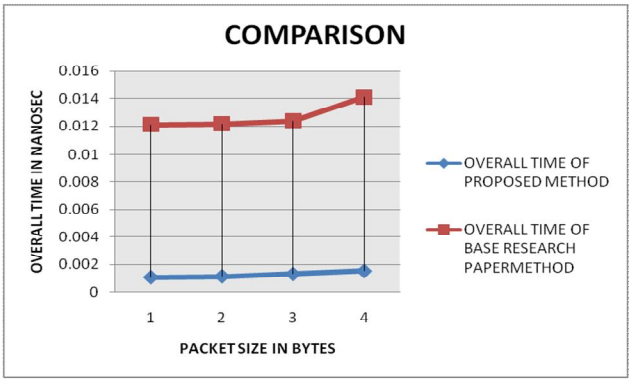

Figure 4 Overall Time Comparison with Both Mechanisms

5. CONCLUSION

In our research we tried to implement a new method in TCP/IP packet transaction. We have showed that it will increase the performance of data transformation. This Method is quiet effective in terms of time taken by Files to

encode as well encrypt as compared to the previous research and effectively improves the bandwidth utilizations and also reduces the traffic of overall network due to small size of packet. The overall performance of the network will increase while implementing compression with cryptography technique. Cryptography technique reduces the hacker intrusion and stealing of data theft. It takes control over the IP spoofing hackers.

6. FUTURE WORK

We have implemented a simple compression algorithm which does not support special symbols in text data or file like (#,$,%) in coding table of bit reduction algorithm. So, better compression algorithm can be defined which efficiently work with NTRU cryptography algorithm with fast access and delivery of packet with security.

References

[1.] S.Gavaskar, Dr.E.Ramaraj, R.Surendiran, "A Compressed Anti IP Spoofing Mechanism Using Cryptography ", *IJCSNS International Journal of Computer Science and Network Security*, VOL.12 No.11, November 2012 .

[2.] Atul Kahate(Novemeber,2010), A Book on Cryptography and Network security,2E.
Avialble online: http://www.mhhe.com/kahate/cns2e.

[3.] Dr. M. Lilly Florence, D.Swamydoss," SECURITY ISSUES IN COMPUTER NETWORK ARCHITECTURE" , *Journal of Global Research in Computer Science*, Volume 2, No. 7, July 2011 .

[4.] Linda S. Rutledge, Lance J. Hoffman," A survey of issues in computer network security", *Journal of Global Research in Computer Science*, Volume 2, No. 7, August 2009.

[5.] Bishop, M, Davis,"what is computer network security", *IEEE Security & Privacy*, Volume 1 , Issue 1 Jan-Feb, 2003

[6.] Debashish Chakraborty, Sandipan Bera , Anil Kumar Gupta, Soujit Mondal," Simple Data Compression by Differential Analysis using Bit Reduction and Number System Theory", *ACEEE Int. Journal on Information Technology*, Vol. 01, No. 03, Dec 2011.

[7.] Agus Dwi, Bali," A New Algorithm for Data Compression Optimization", *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 3, No.8, 2012.

[8.] Mark Daniel Ward ," Exploring Data Compression via Binary Trees", *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 3, No.8, 2012.

[9.] An Article by P.S.Aggarwal on Huffman/Lempel-Ziv Compression Methods on August 2008.

[10.]E. Thambiraja,G. Ramesh,Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue 7, July 2012.

[11.]Bhawana ," An overview and Cryptographic Challenges of RSA", *International Journal of Emerging Research in Management &Technology, Volume-2, Issue-3*.

[12.]Jeff Hoffstein Daniel Lieman Jill Pipher Joseph H. Silverman article on NTRU: A PUBLIC KEY CRYPTOSYSTEM NTRU Cryptosystems, Inc.