# A Compressed Anti IP Spoofing Mechanism Using Cryptography

**S.Gavaskar[1], Dr.E.Ramaraj[2], R.Surendiran[3]**
Research Scholar[1], Technology Adviser[2], Lecturer[3]
[1][2][3]Madurai Kamaraj University, Madurai.

**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 effective method to prevent from the IP spoofing using two way security mechanism compression and encryption. This is our faith this approach minimize the data theft in the form of IP spoofing.

***Keywords:***
*IP spoofing, Compression, Cryptography.*

## I .Introduction:

### A. IP spoofing:

IP Spoofing [3] 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.

### B. Compression:

Basically compression classified into two types

- 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. A picture is converted to a digital file by considering it to be an array of dots, and specifying the color and brightness of each dot. If the picture contains an area of the same color, it can be compressed without loss by saying 200 red dots instead of red dot, red dot, etc red dot.

The original contains a certain amount of information; there is a lower limit to the size of file that can carry all the information. For example, most people know that WinRar produce the compressed ZIP file is smaller than the original file; but repeatedly compressing the file will not reduce the size to nothing, and will in fact usually increase the size.

Lossy compression formats suffer from generation loss: repeatedly compressing and decompressing the file will cause it to progressively lose quality. This is in contrast with lossless data compression. Information-theoretical foundations for lossy data compression are provided by rate distortion theory. Much like the use of probability in optimal coding theory, rate distortion theory heavily draws on Bayesian estimation and decision theory in order to model perceptual distortion and even aesthetic judgment.

- 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. For example, it is

Manuscript received November 5, 2012
Manuscript revised November 20, 2012

used in the popular ZIP file format and in the kernel OS UNIX tool gzip. It is also often used as a component within lossy data compression technologies

Lossless compression algorithms and their implementations are routinely tested in head-to-head existing methods. There are a number of better-known compression existing methods. Some existing methods cover only the compression ratio, so winners in this benchmark may be unsuitable for everyday use due to the slow speed of the top performers. Another drawback of some existing methods is that their data files are known, so some program writers may optimize their programs for best performance on a particular data set. The winners on these existing methods often come from the class of context-mixing compression software.

### C. Cryptography:

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. All over the globe, the laws and regulations concerning cryptography are undergoing a vast change. Legal restrictions on the import and export of cryptographic products are being debated and modified.

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.

## 2. Related Work:

- Border gate way protocol

In this section, we briefly describe a few key aspects of BGP [1]. We model the AS graph of the Internet as an *undirected* graph G = (V, E). Each node v Є V corresponds to an AS, and each edge e (u, v) Є E represents a BGP session between two neighboring ASes u, v Є V. To ease exposition, we assume that there is at most one edge between a pair of neighboring ASes.

Each node owns one or multiple network prefixes. Nodes exchange BGP route updates, which may be announcements or withdrawals, to learn of changes in reach ability to destination network prefixes. A route announcement contains a list of *route attributes* associated with the destination network prefix. Of particular interest to us are the path vector attribute, as path, which is the sequence of ASes that this route has been propagated over, and the local prefix attribute that describes the *degree of local preference* associated with the route. We will use r.as_path, r.local_pref, and r.prefix to denote the as_path, the local_pref, and the destination network prefix of r, respectively. Let r.as_path = (vk, vk-1….v1, v0). The route was originated by node v0, which owns the network prefix r.prefix. Before arriving at node vk, the route was carried over nodes v1, v2… vk-1 in that order. For i = k, k – 1… 1, we say that edge e (Vi, vi-1) is on the AS path, or e (vi, vi-1) 2 r.as_path. When there is no confusion, route r and it's AS path r.as_path are used interchangeably. For convenience, we also consider a specific destination AS d. all route announcements and withdrawals are specific to the network prefixes owned by d. For simplicity, notation d is also used to denote the network 3 Prefixes owned by the AS d. As a consequence, a route r that can be used to reach the network prefixes owned by destination d may simply be expressed as a route to *reach destination* d. Inter domain packet filters also a method of preventing the IP spoofing.

## 3. Proposed Method:

The main objective of IP compression is to avoid the overhead, which provides the bandwidth utilization. The IP header compression work initiated ten years ago but still there is some drawback and problem persists. For handling the packet transformation in effective manner we are moving to IPv6 but the header size will increase in IPv6. To increase the bandwidth utilizations, avoid the network traffic, congestion, collision, we go for compression technique. Basically compression used for minimize the size of file into half. For example if the original file size is 100mb after compression it will reduced into 50mb. While decompress your file we have to get original information without loose anything. Basic idea behind in this is remove the unwanted data's or information's.

In our work we incorporate the compression technique into TCP/IP packets. While data transfer two end systems will make the communication between these two end points the session will allocated for temporarily. Both systems has an unique IP address for identifying the system in network, using this IP address only communication will established. After establishing the end to end point connection the corresponding application will take charge to transactions. Application will identified using the port number. While continues data transfer some information will repeatedly send to the receiving end namely IP address of sender and receiver, port address of sender and receiver. To avoid this kind of information we go for compression technique. Most of the data compression algorithms have been developed and programmed in the traditional way. None of the previous algorithms has been evolved. The use of Evolutionary Computation has not been thoroughly investigated thus far. Researchers in the compression field tend to develop algorithms that work with specific types of data, taking the advantage of any available knowledge about the data. It is difficult to find a universal compression algorithm that performs well on any data type

**Algorithm:**

- Split the packet header with data
- Applied the GRS compression algorithm
- Apply the cryptography technique
- Transmit the data
- Decryption
- Decompression
- Original information.

First take the original packet then split the packet header with the data. Whenever the data transmission happen that time 4tuple information are common for through out the data transfer. If we compress these things we can minimize the many space due to that we can utilize bandwidth in optimized manner.

The next step is applying the GRS algorithm which is the novel algorithm what we designed for our implementation. The concept behind in this is group of IP address considered as a single no which is taken as host identification no like wise we have to interchange into 4tuple's. For example 192.168.30.2 this is a one host IP address. This will converted into like this. 2. We have to remember one thing after establishing the connection only the stream of packet will change into like this.

The next step is applying the cryptography technique. There are variety of techniques and complex methods available but in this scenario we couldn't use the complex technique because we going to apply in packet header. If we use complex technique, for encryption and decryption will take too much time. We have to use simple functions; in our implementation we used transformation function as method. It just modify the one value into another form using add or multiply that value into original no. for example the previous 2 will converted onto 6 adding 4 with 2 . The final thing is we have to send the key value for decryption. Key value will add into encrypted value for easy identification similar to the format of IP address 6.4 is the final value that will send to the destination machine like wise all 4tuple's. Again the decryption will happen in reverse manner.

## 4. Result Analysis:

We have carried out simulation using network simulators. The performance graph shown below describe the how is our method provide the effective fault tolerance, control the traffic and collision.

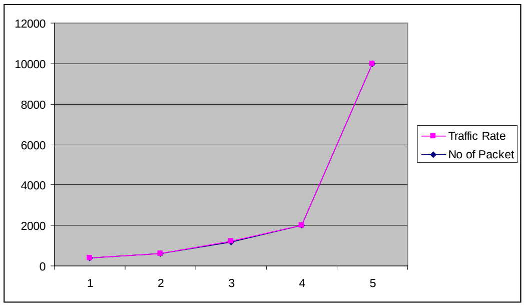

Fig: 1 Normal TCP method

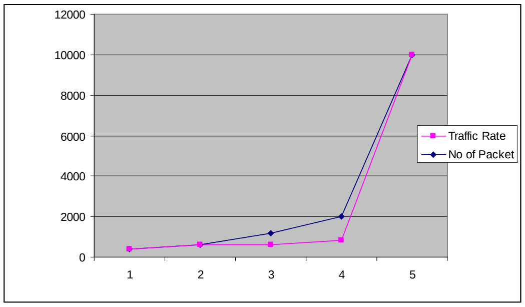

Fig: 2 compressed method

## 5. Future work

In our implementation has taken in IPv4. Now we are working towards IPv6 to implement our concept. Compare with IPv4, IPv6 has large size of packet header if we implement in our technique into IPv6 we will obtain many benefits.

## 6. Conclusion

In our research we tried to implement a new method in TCP/IP packet transaction. It's our faith it will increase the performance of data transformation. This method 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.

## References

[1] Controlling IP Spoofing Through Inter-Domain Packet Filters Zhenhai Duan, *Member, IEEE*, Xin Yuan, *Member, IEEE*, and Jaideep Chandrashekar, Member, IEEE

[2] Improvements on IP Header Compression-C´edric Westphal

[3] Spoofing Prevention Method- Anat Bremler-Barr Hanoch Levy

[4] Stable internet routing without global coordination- L. Gao and J. Rexford,, IEEE/ACM Transactions on Networking, vol. 9, no. 6, Dec.2001.

[5] On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets- K. Park and H. Lee, In Proc. ACM SIGCOMM, San Diego, CA, Aug. 2001.

[6] An introduction to IP header compression published by - WWW. EF FN ET. C OM

[7] Cisco Content Services Switch SSL Configuration Guide-CSS Compression Overview.