Research Article Impact Factor: 0.621 ISSN: 2319-507X
PP Khobragade, IJPRET, 2014; Volume 2 (9): 232-241 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

DATA HIDING USING STEGONOGRAPHY

MS. P. P. KHOBRAGADE[1], DR. H. R. DESHMUKH[2], A. S. MAHALLE[3], S. A. KARALE[4]

1. P. G. Student, IBSS College of Engineering, Amravati.
2. Prof. & Head, IBSS College of Engineering, Amravati.
3. Assistant Professor, IBSS College of Engineering, Amravati.
4. M. E. , IBSS College of Engineering, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: We consider the problem of detecting whether a compromised router is manipulating its stream of packets. In particular, we are concerned with a simple yet effective attack in which a router selectively drops packets destined for some victim. Unfortunately, it is quite challenging to attribute a missing packet to an action because normal network congestion can produce the same effect. Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities. Previous detection protocols have tried to address this problem with a user-defined threshold: too many dropped packets simply intent. We are going to design, an application to detect and recover data packet losses.

Keywords: Packet loss, Stegonography, Man in the Middle Attack, LSB

PAPER-QR CODE

Corresponding Author: MS. P. P. KHOBRAGADE

Access Online On:

www.ijpret.com

How to Cite This Article:

PP Khobragade, IJPRET, 2014; Volume 2 (9): 232-241

INTRODUCTION

Packet loss is a set of programs to detect packet losses in between two hosts. It does this by sending a continuous stream of packets, and detects any delay or loss in the streams. It is useful to measure the impact of failover tests. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is distinguished as one of the three main error types encountered in digital communications; the other two being bit error and spurious packets caused due to noise.

Packet loss can be caused by a number of factors including signal degradation over the network medium due to multi-path fading, packet drop because of channel congestion, corrupted packets rejected in-transit, faulty networking hardware, faulty network drivers or normal routing routines . There are two types of attacks:

a) Persistent - attack every connection between two TCP end.

b) Intermittent - attack some of the connections

e.g., 1 of every 5 connections

The main intention of our application is to detect data packet losses and to recover it. Packet loss occurs in every kind of network. All network protocols are designed to cope with the loss of packets in one way or another. But when any external attacker attacks on senders data it is difficult to recover it. In this project we are designing such application in which we can detect the corrupted data and original data will reaches to the destination safely by using the concept of stegonography [18]

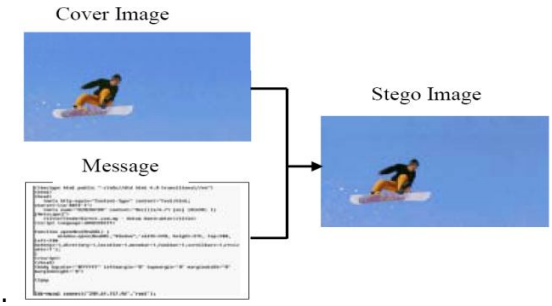


Fig. 1. Producing Stego-Image Process

Stegonography is the efficient technique to provide secure data transmission over the network, as the number of users increases effectively. The cryptography is also used to provide security to data over network, but transmission of secured message may be detectable to third party.

From security point of view, stegonography does not allow to detect the presence of hidden secret other than indeed user, over the communication channel[5].

The proposed method should provide better security while transferring the data or messages from one end to the other end. The main objective of the project is to hide the message or a secret data into an image which acts as a carrier file having secret data and to transmit to the destination securely without any modification. If any distortions occur in the image or on its resolution while inserting the secret message into the image, there may be a chance for an unauthorized person to modify the data. So, the data encryption into an image and decryption and stegonography plays an important role in this project.

I. RELATED WORK

Packet loss occurs in every kind of network. All network protocols are designed to cope with the loss of packets in one way or another. TCP protocol, for example, guarantees packet delivery by sending re-delivery requests for the lost packets. RTP employed by the VoIP protocol does not provide delivery guarantee, and VoIP must implement the handling of lost packet. But when any external attacker attacks on senders data it is difficult to recover it. Whenever sender want to send his data to the receiver due to some reason data is not properly reaches to its destination. There are mainly two reasons which are responsible for improper sending of data packets.

The field of packet loss detection and network security has been around since late 1980s. Since then, a number of methods and frameworks have been proposed and many systems have been built to detect packet loss. Various techniques such as association rules, clustering, naive Bayes classifier, support vector machines, genetic algorithms, artificial neural networks, and others have been applied to detect attacks.

II. EXTERNAL ATTACKS

Packet loss can be caused by a number of factors including signal degradation over the network medium due to multi-path fading, packet drop because of channel congestion[2]. Corrupted packets rejected in-transit, faulty networking hardware, faulty network drivers or normal routing routines[3].The packet loss detector proposed in this paper resembles the idea of the detector used in TCP Vegas[3]. Vegas includes a simple packet loss detector based on delay. On arrival of a dupack, Vegas checks the delay since the transmission of the first unacknowledged packet; if this delay is larger than a fine-grained timeout value (updated every ack), the packet is assumed to be lost, and so is retransmitted. It performs the same test for the first two normal ACKs that arrive after a sequence of dupacks in order to recover from two or three losses which happen close together. They conclude that if losses induced by congestion and

those induced by errors in the wireless link have distinguishable enough statistics, a binary Bayes detector can effectively be used to infer the nature of a packet loss in TCP.

III. ATTACKER CAPABILITIES

The following attacker capabilities define the potential attack scenarios that can be launched from the compromised routers:

The attacker can selectively drop legitimate network traffic, which introduces malicious packet loss behavior by exploiting the congestion control mechanism.

The attacker can send arbitrary network traffic (data and control packets) from the compromised router[15]. The attacker can modify the data packet to introduce anomalous forwarding and routing behavior.

The attacker can physically tamper or remotely access the router to extract secure information from the device.

IV. IMPACTS OF PACKET DROPPING

a) Delay: When we transfer the packet from source to destination, due to congestion or external attacks time delay is occur.

b) Response time: Due to packet dropping response time decreases.

c) Quality: As the time of transmission increases and response time decreases, quality of service reduces.

V. EXISTING SYSTEM

Today, attacker detection is one of the high priority and challenging tasks for network administrators and security professionals. More sophisticated security tools mean that the attackers come up with newer and more advanced penetration methods to defeat the installed security systems. Thus, there is a need to safeguard the networks from known vulnerabilities and at the same time take steps to detect new and unseen, but possible, system abuses by developing more reliable and efficient intrusion detection systems. Any attacker detection system has some inherent requirements. Its prime purpose is to detect as many attacks as possible with minimum number of false alarms, i.e. the system must be accurate in detecting attacks. However, an accurate system that cannot handle large amount of network traffic and is slow in decision making will not fulfill the purpose of an intrusion detection system. We desire a system that detects most of the attacks, gives very few false alarms, copes with large amount of data, and is fast enough to make real-time decisions.

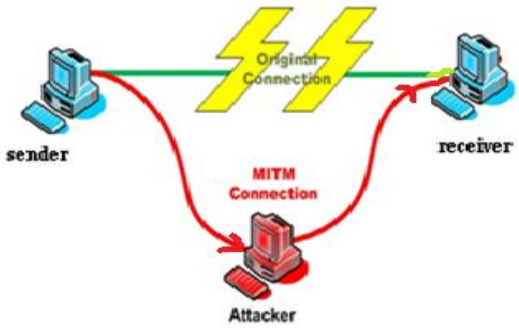


Fig. 3. Attacker Between Connection

In a Man-in-the-Middle attack, an attacker inserts himself between two network nodes. For example, in a successful attack, if Bob sends a packet to Alice, the packet passes through the attacker Eve first and Eve decides to forward it to Alice with or without any modifications; when Alice receives the packet, she thinks it comes from Bob[12]. The attack is bidirectional, so the same scenario applies when Alice sends a packet to Bob. Initially developed to attack public key encryption systems, this attack has expanded to include any form of eavesdropping in which the attacker acts as a proxy and controls the packets exchanged by the two target nodes.

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is distinguished as one of the three main error types encountered in digital communications; the other two being bit error and spurious packets caused due to noise. When any data is transmitted from sender to receiver, if any packet drop or congestion is occur then receiver receives incorrect data but sender and receiver both are unaware about that[13]t. Packet loss can be caused by a number of factors including signal degradation over the network medium due to multi-path fading, packet drop because of channel congestion, corrupted packets rejected in-transit, faulty networking hardware, faulty network drivers or normal routing routines.

When caused by network problems, lost or dropped packets can result in highly noticeable performance issues or jitter with streaming technologies, voice over IP, online gaming and video conferencing, and will affect all other network applications to a degree. However, it is important to note that packet loss does not always indicate a problem. If the latency and the packet loss at the destination hop are acceptable then the hops prior to that one don't matter. Some network transport protocols such as TCP provide for reliable delivery of packets. In the event of packet loss, the receiver asks for retransmission or the sender automatically resends any segments that have not been acknowledged. Although TCP can recover from packet loss, retransmitting missing packets causes the throughput of the connection to decrease. This drop

in throughput is due to the sliding window protocols used for acknowledgment of received packets. In certain variants of TCP, if a transmitted packet is lost, it will be re-sent along with every packet that had been sent after it. This retransmission causes the overall throughput of the connection to drop. Protocols such as UDP provide no recovery for lost packets. Applications that use UDP are expected to define their own mechanisms for handling packet loss.

VI. DISADVANTAGES OF EXISTING SYSTEM

Low packet loss rates usually produce same perception as high delays. However packet loss turns into a bigger issue with video applications such as streaming and videoconferencing. Large delays cause frustration to web users. On business-to-consumer applications this directly affects the actual sales rates.

It severely impacts the perceived quality of voice communication and leads users to shorten voice calls. Finally it results in very noticeable performance problems with gaming applications.

VII. PROPOSED SYSTEM

We are going to design an application for detecting packet losses which inform sender that sent data is corrupted. In this case, the users cannot access their applications anymore until a manual action is executed on the equipments to restore the function of the network. But in our application we can easily detect the packet loss. In proposed system we use stegonography concept based on LSB (Least Significant Bit)algorithm for sending data towards the receiver. we can retransmit the same packet towards the receiver if this stegonography technique fails.

As soon as attacker attacks on data immediately sender and receiver knew about the attack. Due to the reduction of time delay quality of service also increases. We can transmit original data to the receiver safely.

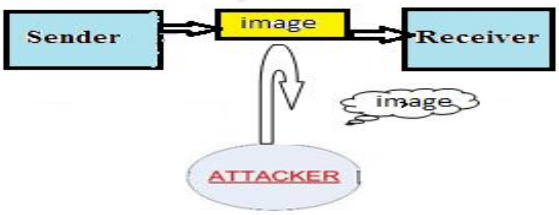


Fig 4 : Securely transmission of data

The block diagram for stegonography technique is as follows.

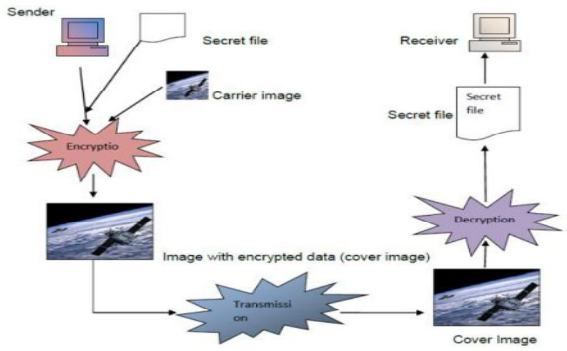
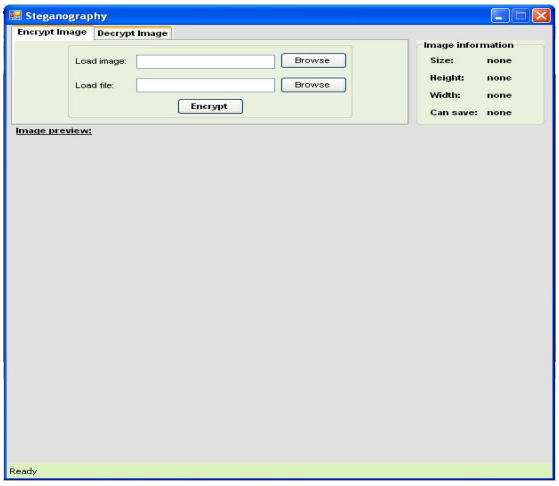


Fig 5: Block diagram for Stegonography

The procedure for data hiding using stegonography algorithm is as follows:

1) The sender first uses the stegonography algorithm for encrypting the secret message.
2) For this encryption, the sender uses any text documents or audio or video files in which the data is written and the image file as a carrier file in which the secret message or text document or audio or video file to be hidden.
3) The sender sends the carrier file and text document or audio or video file to the encryption phase for data embedding, in which the text document or audio or video file is embedded into the image file.



In encryption phase, the data is embedded into carrier file which was protected with the password. Now the carrier file acts as an input for the decryption phase. The image in which data is hidden i.e. the carrier file is sent to the receiver using a transmission medium. E.g. Web or e-mail. The receiver receives the carrier file and places the image in the decryption phase. In the decryption phase, the original text document or audio or video file can be revealed using the appropriate password. The decryption phase decrypts the original text document or audio

or video file using the least significant bit decoding and decrypts the original message. As mentioned in the above block diagram, the data hiding and the data extracting will be done in three phases[19].

1) Encryption Phase: The "Encryption phase" uses two types of files for encryption purpose. One is the secret file which is to be transmitted securely, and the other is a carrier file such as image. In the encryption phase the data is embedded into the image using "Least Significant Bit algorithm" (LSB) by which the least significant bits of the secret document are arranged with the bits of carrier file such as image, Such that the message bits will merge with the bits of carrier file. In this procedure LSB algorithm helps for securing the originality of image.

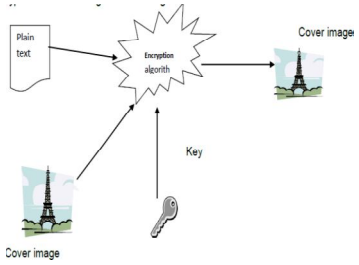


Fig 6: Encryption phase

2) Transmission Phase: The transmission phase is one of the important sections for sending the data to destination securely.

3) Decryption Phase: The Decryption phase is reverse to encryption phase. In decryption phase, the carrier image in which the data is hidden is given as an input file. The decryption phase uses the same password which was given for the encryption and decryption in order to secure from unauthorized access. After giving the correct password the decryption section uses the "Least Significant bit Algorithm" (LSB) by which the encoded bits in the image is decoded and turns to its original state and gives the output as a text document or audio or video file as well as image.

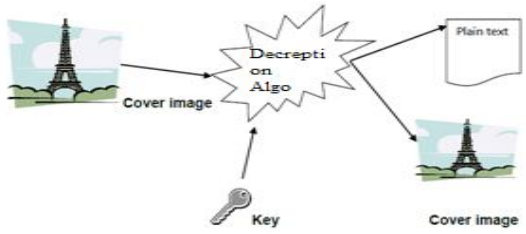


Fig 7: Decryption Phase

VIII. APPLICATIONS

1. Enables secret communication

2. Complements regular encryption: Harder to break: need to first find the encrypted secret text then it needs to be decrypted

3. Tremendous use in Military Applications

REFERENCES

1. Kurose, J. F. & Ross, K. W. (2010). Computer Networking: A Top-Down Approach. New York: Addison-Wesley. P 30.

2. Perkins, C. E. (2001). Ad-Hoc Networking. Boston: Addison-Wesley. P 147.

3. Overview of Attack Trends, http://www.cert.org/archive/pdf/attack_trends.pdf, 2002.

4. "Packet loss or latency at intermediate hops." (HTTP). Retrieved 2007-02-25.

5. A. Tacticus, How to survive under siege / Aineias the Tactician, pp. 84{90, 183{193. Clarendon ancient history series, Oxford, England: Clarendon Press, 1990, ISBN 0-19-814744-9,translated with introduction and commentary by David Whitehead.

6. Mansfield, K. C. & Antonakos, J. L. (2010).Computer Networking from LANs to WANs: Hardware, Software, and Security. Boston: Course Technology, Cengage Learning. P501.

7. Kurose, J. F. & Ross, K. W. (2010). Computer Networking: A Top-Down Approach. New York: Addison-Wesley. P 282-283

8. Kurose, J. F. & Ross, K. W. (2010). Computer Networking: A Top-Down Approach. New York: Addison-Wesley. P 30.

9. Kurose, J. F. & Ross, K. W. (2010). Computer Networking: A Top-Down Approach. New York: Addison-Wesley. P 282-283

10. V. Paxson and M. Allman, “Computing tcp’s retransmission timer,”2988

11. J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of tcp reno congestion avoidance and control," U. Massachusetts Amherst Dept. of Computer Science, Tech. Rep., 1999.

12. L. S. Brakmo, S. W. O'Malley, and L. L. Peterson, "Tcp vegas: new techniques for congestion detection and avoidance," in Proceedings of the conference on Communications architectures, protocols and applications. ACM Press, 1994, pp. 24–35.

13. J. Liu, I. Matta, and M. Crovella, "End-to-end inference of loss nature in a hybrid wired/wireless environment," in Proceedings of WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2003.

14. D. Barman and I. Matta, "Effectiveness of loss labeling in improving tcp performance in wired/wireless networks,".