International Journal of Electrical and Electronic Engineering & Telecommunications

ISSN 2319 – 2518 www.ijeetc.com
Special Issue, Vol. 1, No. 1, March 2015
National Level Technical Conference P&E- BiDD-2015

Research Paper

DETECTION MONITORING OF SECURE PACKET TRANSFER OVER NETWORK TRAFFIC

Gobika S[1]*, Janane T K[1], Mohana Priya U[1] and C Gnanaprakasam[1]

*Corresponding Author: Gobika S, ✉ sgobika@jeppiaarinstitute.org

In the world of Networks, Everything on the Internet involves packets. Web page constitutes of a series of packets, and every e-mail get transfers as a series of packets. In the proposed methodology, a monitoring system has been designed for tracing the packet transfer between the source and destination. A strategy of pattern matching has been utilized to monitor the source and destination content for its originality based on the water marking security concepts. In the proposed methodology, the monitoring system has been designed with leakage analyser for checking the intrusion or leakage of packets between the transfers of source to destination. A security based packet tracing has been designed and the performance of the monitoring system has been visualized graphically.

Keywords: Secure packet transfer, Network traffic, Leakage analyser

INTRODUCTION

Network Security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access network.

Security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a

[1] Department of IT, Jeppiaar Institute of Technology, Chennai, India.

corresponding password. An observation system has been designed for tracing the packet transfer between the source and destination. A strategy of pattern matching has been utilised to watch the supply and destination content for its originality supported the water marking security ideas. In the projected methodology, the observation system has been designed with leak analyser for checking the intrusion.

EXISTING SYSTEM

The conventional systems maintain high detection accuracy while coping with some of the traffic variation in the network (e.g., network delay and packet loss), however, their detection performance substantially degrades owing to the significant variation of video lengths.

In this paper, we focus on overcoming this issue by proposing a novel content-leakage detection scheme that is robust to the variation of the video length.

By comparing videos of different lengths, we determine a relation between the length of videos to be compared and the similarity between the compared videos.

Therefore, we enhance the detection performance of the proposed scheme even in an environment subjected to variation in length of video.

Through a test bed experiment, the effectiveness of our proposed scheme is evaluated in terms of variation of video length, delay variation, and packet loss.

Demerits

Packets loss is a major problem in the existing system. Delay in data sharing while sending packets from source to destination.

The contributions in solving these problems are:

- Sender in an application, used to send the content with watermarking information.
- To enhance the process, we are using monitoring system to detect the Content leakage and intrusion.
- Once monitored the content leakage and intrusion in an application, each and every content is transferred as packet.
- While packet transfer there is no intrusion or defect in a content.
- It checks the originality of the content after packet transferred from a monitoring system not only the original content also with watermarked content.
- Monitoring system analyse the originality of the content and it is time consuming while transferring packets.
- These contents along with watermarked source send to the receiver through monitored system only.

Merits

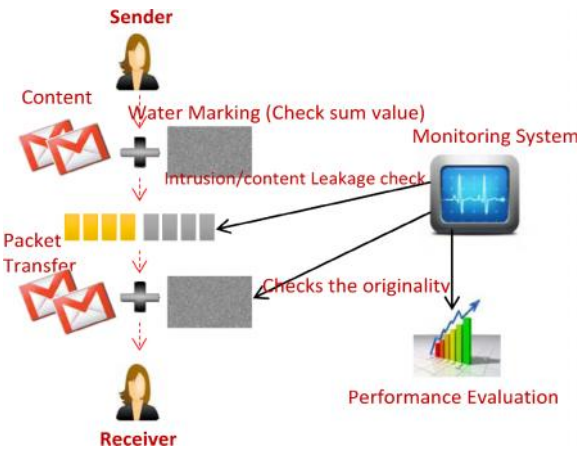
- Monitoring system is there to check out the leakage in sending of packets.
- No delay in the packet transfer from source to destination.

LITERATURE REVIEW

Traffic Pattern Based Content Leakage Detection for Trusted Content Delivery Network

Due to the increasing popularity of multimedia streaming applications and services, the issue of trusted video delivery to prevent undesirable content-leakage has become critical. While

Figure 1: Architecture Diagram



preserving user privacy, conventional systems have addressed this issue by proposing methods based on the observation of streamed traffic throughout the network. These conventional systems maintain a high detection accuracy while coping with some of the traffic variation in the network, however, their detection performance substantially degrades owing to the significant variation of video lengths.

In this paper, we focus on overcoming this issue by proposing a novel content-leakage detection scheme that is robust to the variation of the video length. By comparing videos of different lengths, we determine a relation between the length of videos to be compared and the similarity between the compared videos. Therefore, we enhance the detection performance of the proposed scheme even in an environment subjected to variation in length of video. Though a test bed experiment, the effectiveness of our propose scheme is evaluated in terms of variation of video length, delay variation and packet loss.

The content leakage detection system based on the fact that each streaming content has a unique traffic pattern is an innovative solution to prevent illegal re-distribution of contents by a regular, yet malicious user. Though three conventional methods show robustness to delay, jitter or packet loss, the detection performance decreases with considerable variation of video lengths. This paper attempts to solve these issues by introducing a dynamic leakage detection scheme. Moreover, in this paper, we investigate the performance of the proposed method under a real network environment with videos of different lengths. The proposed method allows flexible and accurate streaming content leakage detection independent of the length of the streaming content, which enhances secured and trusted content delivery.

PROPOSED SYSTEM

In the proposed system, the monitoring system has been designed with the leakage analyser for checking the intrusion and the content leakage. If there is no leakage or any intrusion then only the packet is transferred from sender to receiver. It also checks the originality of the content not only the original content but also the watermarking content. If there is any leakage or intrusion attacks then the monitoring system send the alert to the sender and receiver. The performance of the system can be visualized graphically.

IMPLEMENTATION MODULLE

Implementation is the stage of the project when the theoretical design is turned out into a working system.

1. User Detail Module
2. Packet Sharing Module
3. Intrusion Detection Module

4. Information Leakage Module
5. Packet Monitoring Module
6. Performance Evaluation Module

User Detail Module

In the user details module, the inputs from the user will be fetched and stored in the database for the standard for sending the data's from the source to the destination.

Packet Sharing Module

The sender will be sending the packets of data's of information. Every data's from the source is sent via packets to reach the destination of the receiver.

Intrusion Detection Module

In the Intrusion detection module, the loss of packets will be checked and evaluated based on the sent data's of packets transfer. If the data's are lost during packet transfer then obviously, there will be an intruder changing the content in the data packets.

Information Leakage Module

Information will be leaked or changed by the intruder or because of any other reasons will be checked in the information leakage check module. In this module, packets will be checked on the traversal of source to destination of the specified users.

Packet Monitoring Module

The Packet Monitoring Module will be emphasized with the checking up of the data loss during the packet transfer from the sender side to the client side data exchange. Each and every packet is monitored during the packet transfer.

Performance Evaluation Module

The overall performance of the system will be checked and evaluated in the performance evaluation module based on the original packet transfer from the user to the receiver of the traffic.

CONCLUSION

Main goal of this project is evaluation of any network for better performance and security. This means use of system resources like memory and processor must be less, packet loss should be less as compared to other system. This section include various test conducted on data captured from network, these test are conducted on the basic of various parameters. Due to loss and Damage of Data Transmission, We proposed one Concept. In order to overcome that, We Proposed a Technique to Transferring the Image or Video form Source to Destination Without any Loss of Data and Leakage of Data.

FUTURE WORK

In future work, content of packets can be converted in the readable format which helps the administrator to understand the information very easily and we can send the image and videos we can transfer using data transmission without any loss. And also the criteria needed to view the image and video for the paid user required some extended calibrations and dimensions.

REFERENCES

1. Atsushi Asano, Hiroki Nishiyama and Nei Kato (2010), "The Effect of Packet Reordering and Encrypted Traffic on Streaming Content Leakage Detection

(Invited Paper)", International Conference on Computer Communication Networks (ICCCN'2010), August, Zurich, Switzerland.

2. Garcia-Hernandez J J, Nakano M and Perez H (2005), "Real Time Implementation of Low Complexity Audio Watermarking Algorithm", in Proceedings of the 3rd International Workshop on Random Fields and Processing in In Homogeneous Media, October, Guanajuato, Mexico.
3. Golaup A and Aghvami H (2006), "A Multimedia Traffic Modeling Framework for Simulation Based Performance Evaluation Studies", *Computer Network*, Vol. 50, No. 12, pp. 2071-2087.
4. Matsuda K, Nakayama H and Kato N (2010), "A Study on Streaming Video Detection Using Dynamic Traffic Pattern", *IEICE Transactions on Communications (Japanese Edition)*, Vol. J19-B, No. 02.
5. Mizrahi T (2002), "Real-Time Implementation for Digital Watermarking in Audio Signals Using Perceptual Masking", Signal and Image Processing Lab., Dept. of EE, Technion, Tech. Rep.
6. Petitcolas F, Anderson R and Kuhn M (1999), "Information Hiding—A Survey", in *Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Content*, Vol. 87, pp. 1062-1078.
7. Tachibana R (2004), "Sonic Watermarking", *EURASIP Journal on Applied Signal Processing*, pp. 1954-1956.
8. Zhang Y, Ma P and Su X (2009), "Pattern Recognition Using Interval-Valued Intuitionistic Fuzzy Set and Its Similarity Degree", IEEE International Conference on Intelligent Computing and Intelligent Systems.