Secure Content Leakage Detection in Packet Transfer Systems: A Traffic Pattern-Based Approach

Rohan P. Kulkarni, Dr. Pallavi S. Ingole, and Aishwarya R. Jadhav

Department of Computer Science and Engineering, Kavayitri Bahinabai Choudhari North Maharashtra University, Jalgaon, India -425001

ABSTRACT

In recent years, popularity of multimedia streaming applications and services over the Internet has increased where users connect and receive data. Streaming media is the method used to deliver multimedia elements like videos and music to an end user. The issue of trusted content delivery has occurred. In the proposed methodology, a monitoring system has been designed for streamed traffic observation of whole network. This can trace the packet transfer between the source and destination. These conventional systems detect some issues of traffic variation, like network delay and packet loss. Therefore, we enhance the detection performance of the proposed scheme subjected to variation in length of video.

Keywords: *Streaming content, secure packet transfer, leakage detection, degree of similarity.*

I. INTRODUCTION

Due to the increasing popularity of multimedia streaming applications and services, observation of streamed traffic is necessary for security of organizations, enterprises and other types of institutions. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. An observation system has been designed for tracing the packet transfer between the source and destination. To protecting user privacy and prevent undesirable contents distribution to unauthorized users and to protect authors copyrights used digital rights management (DRM) technology, but these approaches have no significant effect on redistribution of contents. In this paper, we focus on the illegal redistribution of streaming content by an authorized user to external networks.

II. DETECTION SYSTEM FOR STREAMING CONTENTS

The Contents Server distributes contents, each user receives contents and each Router observes the amount of traffic. This information is sent to the Management Server which has an authorized users list, a list of users allowed to receive contents. The Management Server constructs server side and user-side traffic patterns from information about the amount of traffic and matches patterns with each other. With matching results at the Management Server, contents streaming of users are detected. This topology consists of two main components, namely the traffic pattern generation engine embedded in each router, and the traffic pattern matching engine implemented in the management server. Therefore each router can observe its traffic volume and generate traffic pattern. Then traffic pattern matching engine computes the similarity between traffic patterns through a matching process, and based on specific criterion, detects contents leakage.

III. PROPOSED SYSTEM

In the proposed system, we focus on the illegal redistribution of streaming content of an authorized user to external networks. The monitoring system has been designed with the leakage analyses for checking the intrusion and the content leakage. It should compare videos file size and different length then determines a relationship between the length of videos to be compared and their similarity. If there is no leakage or an intrusion then only the packet is transferred from sender to receiver. It also checks the originality of the content and also watermarking content. If there is any leakage or intrusion attack then the monitoring system send the alert to the sender and receiver. The performance of the system can be visualized graphically.

Figures:

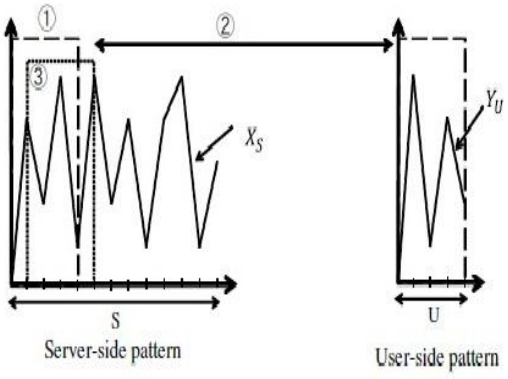

Fig.1. Traffic pattern generation process

A pattern consists of three steps.
1. Window snips off partial pattern X^U.
2. Compare X^U and Y^U.
3. Shift the window by 1 slot and repeat the process from 1 to 3.

SYSTEM ARCHITECTURE:

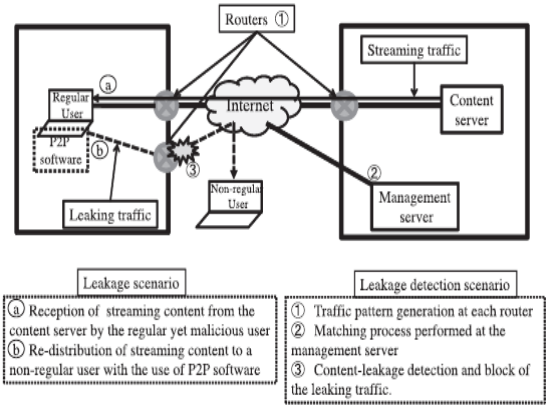

Fig.2. System Architecture of leakage scenario and leakage detection scenario

This topology consists of two main components, namely the traffic pattern generation engine embedded in each router, and the traffic pattern matching engine implemented in the management server. Therefore each router can observe its traffic volume and generate traffic pattern. Meanwhile, the traffic pattern matching engine computes the similarity between traffic patterns through a matching process, and based on specific criterion, detects contents leakage.

IV. ENHANCEMENT OF DETECTION TECHNIQUE

To handle the different Length of Streaming contents we used new threshold determination method based on an exponential approximation. Traffic patterns of streaming videos represent the skeleton carrying their characteristics and are unique per content. Therefore, the longer the traffic pattern is, the more information on the video it displays. In conventional methods, it is assumed that a certain length of content can always be obtained through the network

for all contents. Therefore it is possible to utilize a fixed decision threshold. If there is different length of contents network environment then also leakage detection is possible.

V. CONCLUSION

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. Though conventional methods, Show robustness to delay, jitter or packet loss, the detection performance drops with considerable variation of video lengths. This system tries to solve these issues by introducing a dynamic leakage detection scheme.

REFERENCES

1. *Y. Chu, S. G. Rao, S. Seshan and H. Zhang, "Enabling conferencing applications on the Internet using an overlay multicast architecture," in Proc. ACM SIGCOM, pp.55-67, California, USA, Aug. 2001.*
2. *Z. Yang, H. Ma, and J. Zhang, "A dynamic scalable service model for SIP-based video conference," in Proc. 9th International Conference on Computer Supported Cooperative Work in DE..*
3. *E.I. Lin, A.M. Eskicioglu, R.L. Lagendijk, and E.J. Delp, "Advances in digital video content protection," Proc. IEEE, vol.93, no.1, pp.171-183, Jan. 2005.*
4. *K. Matsuda, H. Nakayama, and N. Kato, "A Study on Streaming Video Detection using Dynamic Traffic Pattern," IEICE Transactions on Communications (Japanese Edition), vol.J19-B, no.02, 2010.*
5. *S. Amarasing and M. Lertwatechakul, "The Study of Streaming Traffic behavior," KKU Engineering Journal, vol.33, no.5, pp.541-553, Sept.- Oct. 2006.*
6. *D. Geiger, A. Gupta, L. A. Costa, and J. Vlontzos, "Dynamic Programming for Detecting, Tracking, and Matching Deformable Contours," in Proc. IEEE Transactions on Pattern Analysis and Matchine Intelligence, vol.17, no.3, pp.294-302, Mar. 1995.*