International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-2, May 2015
ISSN: 2395-3470
www.ijseas.com

The Effect of Packet Reordering and Encrypted Traffic on Streaming Content Leakage Detection

B.Praveena , S.Rajiya sulthana

CSE,BCETW,KADAPA , AP, INDIA

CSE,BCETW,KADAPA , AP, INDIA

Abstract

Due to the increasing popularity of multimedia streaming applications and services in recent years, the issue of trusted video delivery to prevent undesirable content-leakage has, indeed, become critical. While preserving user privacy, conventional systems have addressed this issue by proposing methods based on the observation of streamed traffic throughout the network. we focus on overcoming this issue by proposing a novel content-leakage detection scheme that is robust to the variation of the video length. Through a testbed experiment, the effectiveness of our proposed scheme is evaluated in terms of variation of video length, delay variation, and packet loss.

Keywords: Streaming content, leakage detection, traffic pattern, degree of similarity.

1.INTRODUCTION

A crucial concern in video streaming services is the protection of the bit stream from unauthorized use, duplication and distribution. One of the most popular approaches to prevent undesirable contents distribution to unauthorized users and/or to protect authors' copyrights is the digital rights management (DRM) technology. On the other hand, packet filtering by firewall-equipped egress nodes is an easy solution to avoid leakage of streaming contents to external networks. we focus on the illegal redistribution of streaming content by an authorized user to external networks. The retrieved information are used to generate traffic patterns which appear as unique waveform per content just like a fingerprint. developing an innovative leakage detection method robust to the variation of video lengths is, indeed required. In this paper, by comparing different length videos, we determine a relationship between the length of videos to be compared and their similarity.

2.EXISTING SYSTEM

A crucial concern in video streaming services is the protection of the bit stream from unauthorized use, duplica-tion and distribution. One of the most popular approaches to prevent undesirable contents distribution to unauthorized users and/or to protect authors' copyrights is the digital rights management (DRM) technology. Most DRM techni-ques employ cryptographic or digital watermark techniques.However, this kind of approaches have no significant effect on redistribution of contents, decrypted or restored at the user-side by authorized yet malicious users.

2.1 PROPOSED SYSTEM

In this paper, we focus on the illegal redistribution of streaming content by an authorized user to external networks.The existing proposals monitor information obtained at different nodes in the middle of the streaming path. The retrieved information are used to generate traffic patterns which appear as unique waveform per content, just like a fingerprint

3.Equations:

$$X_N = (x_1, x_2, \ldots, x_N)^T,$$

$$X'_U = \begin{pmatrix} (x_1 - \overline{x})/s_x \\ (x_2 - \overline{x})/s_x \\ \vdots \\ (x_U - \overline{x})/s_x \end{pmatrix}, \qquad Y'_U = \begin{pmatrix} (y_1 - \overline{y})/s_y \\ (y_2 - \overline{y})/s_y \\ \vdots \\ (y_U - \overline{y})/s_y \end{pmatrix},$$

$$R_{X_U Y_U} = \frac{X'^t_U Y'_U}{\sqrt{\|X'_U\|^2 \|Y'_U\|^2}}, \qquad -1 \le R_{X_U Y_U} \le 1.$$

Another pattern matching algorithm is the dynamicprogramming (DP) matching based on the DP technique[18], [19]. DP matching utilizes the distance [20] between thecompared patterns in U-dimensional vector space as metricrepresenting their similarity.

4.Figures and Tables:

4.1 figures

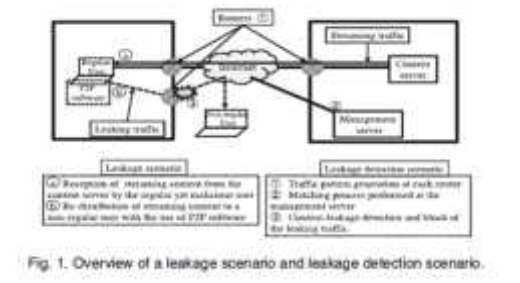

Fig. 1. Overview of a leakage scenario and leakage detection scenario.

4.2 Tables

Comparison of Existing Leakage Detection Methods

T-TRAT	Flow size-based	Data-correlation matching	Dynamic (Gaussian) based	-
P-TRAT	Packet size-based	DP matching	Static (fixed value)	Delay, jitter, packet loss
DP-TRAT				

4.Conclusion:

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 redistribution of contents by a regular, yet malicious user.Though three typical conventional methods, namely, T-TRAT, P-TRAT,and DP-TRAT, show robustness to delay, jitter or packet loss, the detection performance decreases with considerable variation of video lengthsMoreover, 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.

References

Journal papers:

Z. Yang, H. Ma, and J. Zhang, “A Dynamic Scalable Service Model for SIP-Based Video Conference,” Proc. Ninth Int’l Conf. Computer Supported Cooperative Work in DE, pp. 594-599, May 2005.

Books:

Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, “Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture,” Proc. ACM SIGCOMM, pp. 55-67, Aug. 2001.

Chapters in Books:

O. Adeyinka, “Analysis of IPSec VPNs Performance in a Multimedia Environment,” Proc. Fourth Int’l Conf. Intelligent Environments,pp. 25-30, 2008.