ISSN NO: 9726-001X
Volume 03 Issue4 0ct 2015

How Packet Reordering and Secure Connections Impact Finding Missing Streaming Content

Sivaji sharma
Mtech,cse,bcetw, india

Abstract

sending data in real time via the internet. The Main Thing That We Do IsTrusted video delivery to stop unwanted material leakage has been an urgent problem in the years since the rise of multimedia streaming apps and services. Traditional systems have proposed solutions to this problem, all of which rely on monitoring data streams over the network while protecting users' anonymity. To address this problem, we propose a unique content- leaking detection technique that is insensitive to the actual duration of the movie being examined. The efficiency of our suggested approach is measured in terms of video length fluctuation, latency variation, and packet loss through a testbed experiment.

Streaming media, leakage detection, user behavior, and similarity level are some relevant topics to consider.

1.INTRODUCTION

Safeguarding the bit stream against theft, copying, and dissemination is a major issue for video streaming services. Digital rights management (DRM) technology is widely used as a means to restrict access to inappropriate material, safeguard intellectual property rights, and/or both. To prevent the unauthorized redistribution of streaming material by an authorized user to external networks, packet filtering by firewall-equipped egress nodes is a simple solution. The data are utilized to create traffic patterns, which look like a fingerprint in the form of a distinctive waveform for each piece of content. It is necessary to create a novel leakage detection technology that can withstand the wide range in video durations. In this study, we establish a correlation between the duration of the movies being compared and their degree of resemblance.

2.EXISTING SYSTEM

The prevention of illegal copying, sharing, and broadcasting of video streams is a major issue for streaming services. Digital rights management (DRM) technology is widely used as a means to restrict access to inappropriate material, safeguard intellectual property rights, and/or both. Most digital rights management methods make use of cryptographic or digital watermarking methods.Redistribution of materials, decrypted or restored on the user side by authorized but malevolent users, is unaffected by this kind of technique.

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 informationobtained 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:

ISSN NO: 9726-001X
Volume 03 Issue4 0ct 2015

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

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

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

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-dimensionalvector space as metricrepresenting their similarity.

4.Figures and Tables:

4.1 figures

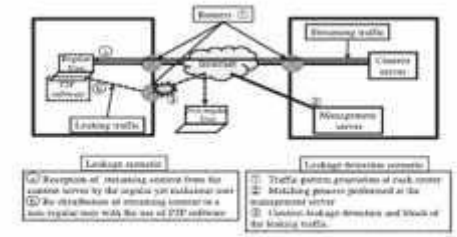

Fig. 1. Overview of a leakage scenario and leakage detection scenario.

4.2 Tables

Comparison of Existing Leakage Detection Methods

4.Conclusion:

To stop the unauthorized sharing of material by a typical but evil user, a new technology has been developed to identify leaks in the content based on the fact that every kind of streaming video has its own distinct traffic pattern.The detection performance degrades with significant variation in video durations, despite the fact that three standard methods—T-TRAT, P-TRAT, and DP-TRAT—show resilience to delay, jitter, or packet loss.Moreover, we examine how the suggested technique fares in a real-world network setting using movies of varying durations in this research. Secure and reliable content delivery is improved by the suggested approach, which enables precise and versatile leakage detection of streaming material regardless of the duration of the streaming content.

References Journal papers:

Published in the proceedings of the Ninth International Conference on Computer Supported Cooperative Work in DE (pp. 594-599), May 2005. Authors: Z. Yang, H. Ma, and J. Zhang.

Books:

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

Book Sections:

Analysis of IPSec VPNs Performance in a Multimedia Environment, O. Adeyinka, Proceedings of the Fourth International Conference on Intelligent Environments, 2008, pp. 25-30.