International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Review Article

A Review on Various Approaches for Detecting and Preventing Content Leakage using Traffic Pattern of Transmission

Sneha U. Agalawe†* and Nitin Chopde†

†Computer Science and Engineering Department, SGBAU, India

Accepted 22 March 2015, Available online 29 March 2015, **Vol.5, No.2 (April 2015)**

Abstract

As the rapid development of broadband technologies and the advancement of high-speed networks, the video streaming applications and service's popularity over the Internet has increased. The protection of the bit stream from unauthorized use, duplication and distribution is the key concern in video streaming services. Digital Rights Management (DRM) is one of the most popular approaches to prevent undesirable contents distribution to unauthorized users but it have no significant effect on redistribution of contents, decrypted or at the user-side by authorized yet malicious users and content leakage. Also preserving user privacy, conventional systems have addressed this issue by proposed methods based on the observation of streamed traffic throughout the network. These conventional systems maintain high detection accuracy while coping with some of the traffic variation in the network. However, the detection performance considerably degrades due to the significant variation of video lengths. This work proposes a content-leakage detection scheme that is robust to the variation of the video length. By comparing videos of different lengths, a relation between the length of videos to be compared and the similarity between the compared videos is determined. Therefore, the detection performance of the proposed scheme even in an environment subjected to variation in length of video will enhance. The effectiveness of proposed scheme is evaluated in terms of variation of video length, delay variation, and packet loss. Also, increased in bandwidth, which enhance the performance of transmission, include a module to enhance the performance of overall system.

Keywords: *Content-leakage, Traffic pattern*

1. Introduction

In recent years, with the rapid advance in broadband technology, digital contents delivery applications have been used widely. The streaming technology has made the contents delivery more popular. Due to the increasing popularity of multimedia streaming applications and services, the issue of trusted video delivery to prevent undesirable content-leakage has, indeed, become critical .The popularity of real-time video streaming applications and services over the Internet has increased by leaps and bounds. A huge population of users from all around the world with diverse contents, ranging from daily news feeds to entertainment feeds including music, videos, sports, and so forth is served, by using streaming transmission technologies. Also, with virtual private networks (VPNs), real-time video streaming communications such as web conference in intra company networks or via Internet are being widely deployed in a large number of corporations as a powerful means of efficiently promoting business activities without additional costs. Rather than packet filtering by firewall-equipped way out nodes is an easy solution to avoid leakage of streaming contents to external networks. In this solution, the packet header information that is destination and source Internet protocol addresses, protocol type, and port number of outgoing traffic, of every streamed packet is inspected.

In case the inspected packets do not verify the predefined filtering policy, they are blocked and dropped. It is difficult to entirely prevent streaming content leakage by means of packet filtering alone because the packet header information of malicious users is unspecified beforehand and can be easily spoofed. The existing proposals monitor information obtained at different nodes in the middle of the streaming path.

The retrieved information is used to generate traffic patterns which appear as unique waveform per content just like a fingerprint. The generation of traffic pattern does not require any information on the packet header, and therefore preserves the user's privacy. Leakage detection is then performed by comparing the generated traffic patterns. In this paper, the focus is on the illegal redistribution of streaming content by an authorized user to external networks.

*Corresponding author: **Sneha U. Agalawe**

2. Literature Survey

In 2014, Hiroki Nishiyama, Desmond Fomo, Zubair Md. Fadlullah and Nei Kato,Fellow proposed a paper on "Traffic Pattern-Based Content Leakage Detection for Trusted Content Delivery Networks". There is no requirement of any information on the packet header in the generation of traffic pattern, and therefore preserves the user's privacy. The detection of leakage is then performed by comparing the generated traffic patterns. However, in the leakage detection performance, the existence of videos of different length in the network environment causes a considerable degradation. Hence, by comparing different length videos, developing an innovative leakage detection method robust to the variation of video lengths is indeed required.

In 2011 ,K. Ramya, D. Ramya Dorai, Dr. M. Rajaram proposed paper on "Tracing Illegal Redistributors of Streaming Contents using Traffic Patterns" .The packet size-based traffic pattern generator adaptation, instead of the time slot based one used in T-TRAT, enables P-TRAT to accomplish robustness to packet delay jitter. The DP matching employment as a pattern matching technique permits DP-TRAT to remove the effect of packet losses. In addition, with significant results on the relations between such algorithms, and the robustness to packet reordering and encryption provides us by their work. However, the important concern in adopting both time slots based and packet size-based traffic generators consisted in the issue of packet reordering, which may have a substantial impact upon the performances of all the conventional methods.(K. Ramya *et al*, 2011)

In 2006 ,S. Amarasing and M. Lertwatechakul proposed a paper on "The Study of Streaming Traffic Behavior," KKU Eng. J., vol. 33, no. 5, pp. 541-553. The understanding of streaming traffic behavior is still advantageous for network system development to capably support streaming traffic in the future. To observe the different traffic behaviors of on-demand traffic (stored-media traffic) and real-time live trafficis the main objective. Moreover, also the study of the relation between encoding bit rates and streaming traffic behavior is carried out.(S. Amarasing *et al*, 2006) In 2006 M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, proposed paper "Traitor Tracing Technology of Streaming Contents Delivery Using Traffic Pattern in Wired/Wireless Environments," propose a system to detect illegal contents streaming by using only traffic patterns which are assembled from the amount of traffic traversing routers. They also investigate a way to cope with random errors and burst errors which occur regularly in wireless environment and show the agreeable result which they have obtained in a practical testing environment.(M. Dobashi *et al*, 2006)

In 1995, D. Geiger, A. Gupta, L.A. Costa, and J. Vlontzos proposed a paper on "Dynamic Programming for Detecting, Tracking, and Matching Deformable Contours" Particular this approach as applied to medical images, the main field of applications considered, was first considered in. The formulation of the cost functions has been subjective by their work. Minimizing an energy function is a typical way to identify deformable shapes. A constraint of this approach has been that the algorithms are slow, iterative, and not guaranteed to discover the global minimum. Moreover, they argue that some of the user input data has not been utilized by previous methods (Y. Chu *et al*).

3. Problem Statement and Discussion

In existing system, the illegal redistribution of streaming content by an authorized user to external networks is focused. The existing proposals display information obtained at different nodes in the middle of the streaming path. The retrieved information are used to create traffic patterns which appear as unique waveform per content , just like a fingerprint. Any information on the packet header is not required for the generation of traffic pattern, and therefore preserves the user's privacy. Leakage detection is then achieved by comparing the generated traffic patterns. However, the presence of videos of different length in the network environment causes a substantial degradation in the leakage detection performance. Thus, developing an innovative leakage detection method stout to the variation of video lengths is, indeed required.

4. Description of the Proposed Work

Streaming contents are sent from the delivery server to the user, and the traffic is witnessed at the server side and the user side. Traffic patterns are then created at the packet observation points and sent to the server, where the matching procedure is performed. To handle variation in network environment such as delay, jitter, and packet loss, we placed the bridge in the middle of the server and the user. P-TRAT- and DP-TRAT based detection performances are used as comparison to our proposed method. These indexes are widely used in recognition techniques and performance calculation of web information retrieval systems. It is worth noting that the larger the accuracy and the recall ratio, the better the leakage detection performance. However, a tradeoff relation exists between the exactness and the recall ratio. We consider both and define their harmonic mean F-measure

The organization of the remainder of the system is as follows: A typical video leakage scenario, detection system and procedures are described. Then, first we illustrate the drawback of the existing scheme due to the variation of video length in realistic environment, then we termed the proposed leakage detection scheme, and we evaluate its calculation cost in judgment to that of the existing scheme. Furthermore, we evaluate the usefulness and the accuracy of the proposed scheme with respect to different length

videos, and its robustness to network environment changes.

Conclusions

The content leakage detection system based on the fact that each streaming content has a inimitable traffic pattern is an innovative solution to prevent illegal redistribution of contents by a regular, yet malevolent user. Though three typical 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. Moreover, we investigate the performance of the proposed method under a network environment with videos of different lengths. The proposed method allows malleable and accurate streaming content leakage detection independent of the length of the streaming content, which enhances secured and trusted content delivery. And also use the conception of bandwidth enhancement for the better performance.

References

Hiroki Nishiyama, Desmond Fomo, Zubair Md. Fadlullah,, and Nei Kato,Fellow,(2014), Traffic Pattern-Based Content Leakage Detection for Trusted Content Delivery Networks, IEEE Transaction on Parallel and Distributed System, Volume 25, No 2

K. Ramya, D. Ramya Dorai, Dr. M. Rajaram (2011) Tracing Illegal Redistributors of Streaming Contents using Traffic Patterns, IJCA

S. Amarasing and M. Lertwatechakul, (2006)The Study of Streaming Traffic Behavior, KKU Eng. J, vol. 33, no. 5, pp. 541-55

M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour,(2006), Traitor Tracing Technology of Streaming Contents Delivery Using Traffic Pattern in Wired/Wireless Environments,Proc. IEEE Global Telecomm. Conf., pp. 1-5.

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.

D. Geiger, A. Gupta, L.A. Costa, and J. Vlontzos,(1995),Dynamic Programming for Detecting, Tracking, and Matching Deformable Contours, Proc. IEEE Trans. Pattern Analysis vol. 17, no. 3, pp. 294-302

R.S. Naini and Y. Wang, (2003)Sequential Traitor Tracing,IEEE Trans. Information Theory, vol. 49, no. 5, pp. 1319-1326

O. Adeyinka,(2008), Analysis of IPSec VPNs Performance in a Multimedia Environment," Proc.Fourth Int'l Conf. Intelligent Environments, pp. 25-30.

A. Asano, H. Nishiyama, and N. Kato, (2010)The Effect of Packet Reordering and Encrypted Traffic on Streaming Content Leakage Detection (Invited Paper), Proc. Int'l Conf. Computer Comm. Networks (ICCCN '10), pp.