ISSN:0975-9646

# Content Leakage Detection by Using Traffic Pattern for Trusted Content Delivery Networks

Miss.V.S.Motade[1], Assoc. Prof. Deepak Gupta[2]

*[1,2]Compuetr Engineering,CAYMET'S*
*Siddhant College of Engineering,*
*Sudumbare, Pune, Maharashtra, India*

*Abstract* - **Multimedia streaming applications and services are becoming popular in recent a year, that's why issue of trusted video delivery to prevent the undesirable content leakage become critical. The conventional Systems addressed this issue by proposing methods based on observation of streamed traffic throughout the network. The job of maintaining high detection accuracy while coping with traffic variation in the network is done by conventional system. But detection performance of conventional system degrades to the significant variation of length of the video. To overcoming this issue we are proposing a novel leakage detection of content scheme that is robust to the variation of the length of the video. In this, we focus on overcoming this issue by proposing a novel content-leakage detection scheme that is robust to the variation of length of the video. By comparing the length of different videos, we determine a relation between video length to be compared and the similarity between the videos which are compared. Thus,we enhance the detection performance of the proposed scheme even in an environment subjected to variation in length of video. Through a experiment, the effectiveness of our proposed scheme is evaluated in terms of variation of video length, variation in delays, packet and data loss.**

**Keywords:** Traffic pattern, Streaming content, leakage detection degree of similarity, multimedia streaming, DRM Technology.

## I. INTRODUCTION

Multimedia streaming applications and services are becoming popular in recent a year, that's why issue of trusted video delivery to prevent the undesirable content leakage become critical. The conventional Systems addressed this issue by proposing methods based on observation of streamed traffic throughout the network. YouTube and Microsoft Network (MSN) video are the examples of such applications. They give a huge population of users from all around the world with contents which are diverse in nature, ranging from daily news to entertainment feeds including audio, videos, music, Matches, sports, and so on, by using streaming transmission technologies. In a real-time video streaming communications such as web conference in intra-company networks or through Internet with Virtual Private Networks (VPNs) are being widely deployed in a large number of corporations as a powerful means of efficiently promoting business activities without additional costs . A crucial concern in video streaming services is the protection of the bit stream from unauthorized use, duplication of bit stream and distribution of content. One of the most popular approaches for the prevention of undesirable contents distribution to unauthorized users and/or to protect authors' copyrights is the Digital Rights Management (DRM) technology. Most DRM techniques use cryptographic scheme or digital watermark techniques. This kind of approaches has no significant effect on re-distribution of contents, decrypted or restored at the user-side by authorized yet malignant users. Moreover, redistribution is technically no longer difficult by using Peer to Peer (P2P) streaming software. Thus, streaming traffic may be leaked to P2P networks. On the other hand, packet filtering by firewall-equipped egress nodes is an easy solution to avoid leakage of streaming contents to external networks. In this solution, the packet header information (e.g., destination and source Internet Protocol (IP) addresses, protocol type, and port number of outgoing traffic) of every streamed packet is inspected. In case the inspected packets do not verify the pre-defined filtering policy, they are blocked and dropped. However, it is difficult to entirely streaming content leakage prevention by means of packet filtering alone because the packet header information of malignant users is unspecified beforehand and can be easily spoofed or sniffed. In this work, focus is on the illegal re-distribution of streaming content by an authorized user to external networks. The existing proposals in monitor information obtained at different nodes in the middle of the path of streaming. The retrieved information is used to generate traffic patterns which appear as unique waveform per content, just like a fingerprint or other biometric devices. The generation of traffic pattern does not require any information on the packet header, and therefore the user's privacy is preserve. Leakage detection is then performed by comparing the generated traffic patterns.

The main idea of paper presented by Hiroki Nishiyama [8] is to detection of content leakage by using traffic pattern. The content leakage detection system based on the fact that each streaming content has a unique traffic pattern is an innovative solution for the prevention of illegal re-distribution of contents by a regular, yet malignant user via three typical Conventional methods, namely T-TRAT, P-TRAT, DP-TRAT, show robustness to delay, packet loss, the detection Performance decreases with considerable variation of lengths of videos. Our approach is to solve these issues by introducing a dynamic leakage detection scheme. We check the performance of the proposed method under a real network environment with videos of different lengths. The proposed method is allowed flexible and accurate streaming content leakage detection independent of the length of the streaming content, which enhances secured and trusted Delivery of content.

## II. LITERATURE REVIEW

Paper presented by Yang-hua Chu[1] introduce the enabling conferencing application on the internet using multicast architecture. In response to scalability and deployment concerns with IP Multicast, they advocated an alternate architecture for supporting group communication applications where all multicast functionality is pushed to the edge. They refer to such architecture as End System Multicast. End System Multicast has several advantages, a key concern is the performance penalty associated with such a design. In this they explore how Internet environments and application requirements can impudence End System Multicast design. They explore these issues in the context of audio and video conferencing. They conduct an extensive evaluation study of schemes for constructing overlay networks on a wide-area test-bed of about 10-20 hosts distributed around the Internet. There results demonstrate that it is most important to adapt to both latency and bandwidth while constructing overlays optimized for conferencing applications. They gives results which indicate that End System Multicast is a variable architecture for enabling performance demanding audio and video conferencing applications in dynamic and heterogeneous Internet settings. In their experiments with our Primary Set, at source rates of both 1.2 and 2.4 Mbps, most hosts are able to sustain over 95% of the source rate on average, and yet achieve latencies of less than 100 ms. In extremely heterogeneous settings such as the Extended Set, the mean performance attained by each receiver is comparable to the performance of the unicast path from the source to that receiver. They gives results indicate that to achieve good performance for conferencing applications, it is critical to consider both bandwidth and latency while constructing overlays.

Paper presented by Karen Su[2] ,In this they present a theoretical framework for the linear collusion analysis of watermarked digital video sequences, and derive a new theorem which equating statistical invisibility, collusion-resistance and two practical watermark rules for design. The proposed framework is simple. The basic processing unit is the video frame and we consider second- order statistical descriptions of their temporal inter-relationships. Within this analytical setup, we define the linear frame collusion attack, the analytic notion of a statistically invisible video watermark, and show that the latter is an attack which is effective against the former. Finally, for showing how the theoretical results detailed in this can easily be applied to the construction of collusion-resistant watermarks of video, they encapsulate the analysis into two practical video watermark design rules that play a key role in the subsequent development of a novel collusion-resistant video watermarking algorithm.

Paper presented by Yong Liu, K. Ramya [3], Video-over-IP applications has recently attracted a large number of users on the Internet. Client server based video streaming solutions incur expensive bandwidth provision cost on the server. Peer-to-Peer (P2P) networking is a new paradigm to build distributed network applications. Recently, severalP2P streaming systems have been deployed to provide live and on demand video streaming services on the Internet at low cost. In this, we provide a survey on the existing P2P solutions for live and on-demand video streaming. Representatives P2P streaming systems, including tree and mesh based systems are introduced. In this they describe the challenges and solutions of providing live and on demand video streaming in P2P environment. In this, we conducted a survey on the existing P2P video streaming technology. They described several key P2P streaming designs, including system topologies and data scheduling, that gives various challenges in providing large scale live and on-demand video streaming services on top of the best-effort Internet. Current Deployments on the Internet demonstrate that P2P streaming systems are capable of streaming video to a large user population at low server cost and with minimal dedicated infrastructure. However, there are several fundamental limitations of existing P2P video streaming solutions. First of all, the user Quality of Experience in current P2P streaming systems are still not comparable to the traditional TV services provided by cable and satellite broadcasting companies. Specifically, P2P streaming users normally experience much longer channel start-up and channel delays. Video playback starts tens of seconds after a user selects a channel. There are also large playback lags among peers. Some peers watch frames in a channel minutes be- hind other peers. Due to the limited peer uploading capacity, most P2P streaming systems only support video rate up to 400kbps. Consequently, users only receive low resolution videos. In addition, the video streaming quality is poor and unstable when the number of peers watching the same program is small. This makes it challenging to serve long-tailed unpopular contents in P2P streaming systems. Those issues are interesting and challenging research problems that need to be addressed to make P2P video streaming services a real competitor for traditional broadcast TV services. Secondly, the increasingpopularityofP2P streaming has become a serious concern for ISPs. The huge user base and high traffics volume of P2P streaming systems pose a big challenge on ISPs' network capacities. Most current P2P streaming designs are not ISP-Friendly. The peering connections and data exchanges among peers are mostly driven by content availabilities. After peers obtain some video data from the source server, they randomly connect to multiple peers, local and remote, and exchange data between different networks. Unregulated P2P video exchanges significantly increase the traffics volume on links within and between ISPs. As a result, the video content distribution cost is essentially shifted to ISPs without any profit for them. How ISPs should manage and regulate the ever increasing P2P video streaming traffics deserves further investigation to maintain the stability of their network infrastructures. Lastly, playing the dual role of network service provider and content service provider, several ISPs have started to provide IPTV services by deploying IP multicast and video proxy servers in their private networks. P2P streaming has been proved to be a scalable streaming solution with low infrastructure requirement. It will be beneficial for ISPs to integrate P2P technology into their IPTV systems to significantly reduce their server and network infrastructure cost. Many interesting research problems need to be addressed to develop an integrated IPTV solution for content providers, network providers and IPTV users.

Paper presented by K. Matsuda[4] introduce that tracing scheme is using similarity of traffic pattern to trace the source of leaks when sensitive or proprietary data is made available to large set of parties. We must implement digital rights management (DRM) to control content spreading and to avoid unintended content use. General tracing methods use either watermarking or cryptographic private or public keys to protect the digitally protected content. In those methods, malicious users can interrupt tracing with illegal process at user side computers. For the prevention of all illegal process at user side, routers should analyze information embedded in to packets which is unrealistic. The proposed method is used to detect illegal content streaming by using only traffic patterns which are constructed from amount of traffic traversing routers. In recent years, the evolution of advanced wired and wireless access networks along with the rapid development of broadband Internet have allowed us to easily utilize real time video streaming applications and services via high-speed networks. YouTube and MSN Video are best examples of such applications, which serve a huge population of users from all around the world with contents which are diverse in nature, ranging from daily news feeds to entertainment feeds including music, videos, sports, and so forth, by using streaming transmission technologies. One of the most popular approaches to prevent undesirable contents distribution to non-licensed users or to protect the author's copyrights is Digital Rights Management (DRM) technology. Traitor is one who is the illegal redistributors of streaming content to non legitimate user. Traitor tracing is technology which enable us to observe users contents streaming and to detect illegal streaming. In general, traitor tracing systems embed copyright notices and server side information into contents, using the digital watermarking technology. Recently, the method which uses cryptographic keys is to detect illegal transfers of contents. However, those methods depend on information embedded into contents, malicious users can interrupt tracing with illegal process at user side computers. To prevent all illegal processes at user side computers, routers should analyze information embedded into packets which is unrealistic because it needs very high computation. Furthermore, observing information in packets may cause problems from the perspective of the protection of personal information. Therefore, we should examine the traitor tracing method which does not use embedded information. Using Variable Bit Rate (VBR), the movies bit rate changes according to the change of scene. When these movies are delivered and played as contents by streaming, the changes of the amount of traffic will appear as a unique waveform on the contents. This server information base waveform can be related to user information which is independent of the movies contents. Therefore, by matching the waveform at the server side and the waveform at the user side, we can detect the reception of the contents. If there is a user who receives the contents without permission, we judge that this is an illegal reception. The proposed method is used to detect an illegal streaming using only the amount of traffic which is observed in very short period of time from the routers located just before the users. This system can be operated with less processing time than packet analysis. Furthermore, it can prevent illegal processes of malicious users efficiently, because no process is needed at user side computers.

Paper presented by Hiroki Nishiyama [8] introduce that 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. These conventional systems maintain a 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. In this they also introduce the traditional content leakage detection and prevention method.

## CONTENT LEAKAGE DETECTION:

In this section, we first take a look at a typical video leakage scenario, and we present an overview of existing traffic pattern based leakage detection technologies.

### A. Typical video leakage scenario

Due to the popularity of streaming delivery of movies, development of P2P streaming software has attracted much attention. These technologies enhance the distribution of any type of information over the Internet. A typical content leakage scenario can be described. First, a regular user in a secure network receives streaming content from a content server. Then, with the use of P2P streaming software, the regular yet malignant user redistributes the streaming content to a non-regular user outside its network. Such content-leakage is hardly detected or blocked by watermarking and DRM based techniques.

### B. Leakage detection procedures

Throughout the video streaming process, the changes of the amount of traffic appear as a unique waveform specific to the content. Thus by monitoring these information retrieved at different nodes in the network, content-leakage can be detected. An overview of the network topology of the proposed leakage detection system is shown. 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. The result is then notified to the target edge router in order to block leaked traffic.

### C. Pattern generation algorithm

Here, we describe the traffic pattern generation process performed in conventional methods. Traffic pattern generation process is based on a either time slot-based algorithm or a packet size-based algorithm. Packet size-based algorithm defines a slot as the summation of amount of arrival traffic until the observation of a certain packet size. This algorithm only makes use of the packet arrival order and packet size, therefore is robust to change in environment such as delay and jitter. However, packet size based algorithm shows no robustness to packet loss.

### D. Pattern matching algorithm

In pattern recognition, the degree of similarity is defined to be the similarity measure between patterns. The server side traffic patterns represents the original traffic pattern and is expressed as XS = (x1; x2; :::; xS)t. The user-side traffic pattern is expressed as YU = (y1; y2; :::; yU)t. Here, S and U are number of slots, and the length of the user-side observation is shorter than that of the server-side, i.e., S > U.

### E. Leakage detection criterion

The cross correlation matching algorithm is performed on both the traffic patterns generated through time slot based algorithm and those generated through packet size based algorithm. The similarity data obtained from the matching of time slot-based generated traffic patterns are considerably small and their distribution is considered to be normally distributed around zero, since the distribution of cross-correlation coefficient values of two random waveforms is approximated to a normal distribution.

## III. Enhancement Of Detection Technique To Handle Video Contents Of Different Lengths

Among the conventional methods, DP-TRAT method shows high robustness to packet delay, jitter, and packet loss. However, the existence of videos of different lengths subjected to time variation in real content delivery environment causes DPTRAT’s accuracy to decrease. In this section, we take a look at the issue caused by the existence of different length videos in network environments. While focusing on DP-TRAT, we introduce a new threshold determination method based on an exponential approximation, and evaluate the computation cost of both the proposed scheme and an eventual enhancement of the previous scheme. 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 in both PTRAT and DP-TRAT methods. However, there is no such guarantee in actual network environments.

## IV Performance Evoluation

In this section, we describe the performance evaluation experiment carried out using a real network environment. We evaluate the effectiveness and the accuracy of the use of a dynamic decision threshold in a network environment with videos of different length. Moreover, we evaluate the robustness of our scheme to network environment changes. The proposed decision threshold determination technique is implemented into the DP-TRAT which employs the packet size-based traffic generation algorithm and the DP-matching algorithm, because DP-TRAT shows high robustness to network environment changes compare to other schemes.

## V Conclusion

The detection of content leakage 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 typical conventional methods, namely T-TRAT, P-TRAT, DP-TRAT, show robustness to delay, data 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.

## Acknowledgement

I would like to express my sincere thanks to my guide Prof.P.B.Kumbharkar for his motivation and useful suggestions which truly helped me in improving the quality of this paper. I take this opportunity to express my thanks to my teacher, family and friends for their encouragement and support.

## 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] K. Su, D. Kundur, and D. Hatzinakos, “Statistical invisibility for collusion-resistant digital video watermarking,” IEEE Trans. Multimedia, vol.7, no.1, pp.43-51, Feb. 2005.

[3] Y. Liu, Y. Guo, and C. Liang, “A survey on peer-to-peer video streaming systems,” Peer-to-Peer Networking and Applications, Vol.1, No.1, pp.18- 28, Mar. 2008.

[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] 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.

[6] O. Adeyinka, “Analysis of IPSec VPNs Performance in A Multimedia Environment,” School of Computing and Technology, University of East London.

[7] 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

[8] Hiroki Nishiyama, "Traffic Pattern Based Content Leakage Detection for Trusted Content Delivery Networks "Member, IEEE, Desmond Fomo, Student Member, IEEE, Zubair Md. Fadlullah, Member, IEEE and Nei Kato, Fellow, IEEE

## AUTHORS

V.S.Motade, M.E.(Comp), Siddhant College of Engineering, Sudumbare, *Pune*

Prof Deepak Gupta, Assoc. Prof ,institute Siddhant College of Engineering, Sudumbare, *Pune*.