ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Traffic Pattern-Based Video Leakage Detection System for Trusted Networks

B.Prasad
HOD,
Department CSE,
Sri Chaitanya Technical Cmapus,
Ibrahimpatnam.

B.Prasad
Associate Professor,
Department CSE,
Sri Chaitanya Technical Cmapus,
Ibrahimpatnam.

C.Archana
P.G Scholar,
Department CSE,
Sri Chaitanya Technical Cmapus,
Ibrahimpatnam.

Abstract:

The rapid development of broadband technologies and the advancement of high-speed networks, the video streaming applications and service's over the Internet have popularly 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:

Streaming content||, —leakage detection||, —traffic pattern||, —degree of similarity||.

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 serve 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, by using streaming transmission technologies. In addition, real-time video streaming communications such as web conference ,in intercompany networks or via 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 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 techniques employ cryptographic or digital watermark technique. 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. Moreover, redistribution is technically no longer difficult by using peer-to-peer (P2P) streaming software. Hence, 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 addresses, protocol type, and port number of outgoing traffic) of every streamed packet is inspected.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In case the inspected packets do not verify the predefined filtering policy, they are blocked and dropped. However, 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. In this paper, we focus on the illegal redistribution of streaming content by an authorized user to external networks. The existing proposals and 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 percontent,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. However, the existence of videos of different length in the network environment causes a considerable degradation in the leakage detection performance.

Thus, 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. Based on this relationship, we determine decision threshold enabling accurate leakage detection even in an environment with different length videos. The remainder of the paper is organized as follows: A typical video leakage scenario, detection system and procedures are described. First we depict the drawback of the existing scheme due to the variation of video length in realistic environment, then we described the proposed leakage detection scheme, and we evaluate its calculation cost in comparison to that of the existing scheme. Furthermore, we evaluate the effectiveness and the accuracy of the proposed scheme with respect to different length videos, and its robustness to network environment changes.

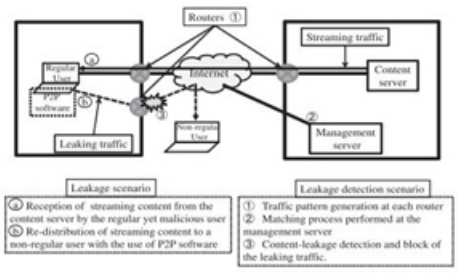

Figure I. Overview of a leakage scenario and leakage detection scenario.

II.RELATED WORK :

Y.Chu, S.G. Rao, S. Seshan, and H. Zhang. In response to the serious scalability and deployment concerns with IP Multicast, we and other researchers have advocated an alternate architecture for supporting group communication applications over the Internet where all multicast functionality is pushed to the edge. We refer to such architecture as End System Multicast. While End System Multicast has several potential advantages, a key concern is the performance penalty associated with such a design. While preliminary simulation results conducted in static environments are promising, they have yet to consider the challenging performance requirements of real world applications in a dynamic and heterogeneous Internet environment. In this paper, we explore how Internet environments and application requirements can influence End System Multicast design.

We explore these issues in the context of audio and video conferencing: an important class of applications with stringent performance requirements. We conduct an extensive evaluation study of schemes for constructing overlay networks on a wide-area test-bed of about twenty hosts distributed around the Internet. Our results demonstrate that it is important to adapt to both latency and bandwidth while constructing overlays optimized for conferencing applications. Further, when relatively simple techniques are incorporated into current self-organizing protocols to enable dynamic adaptation to latency and bandwidth, the performance benefits are significant. Our results indicate that End System Multicast is a promising architecture for enabling performance-demanding conferencing applications in a dynamic and heterogeneous Internet environment.

Z.Yang, H. Ma, and J. Zhang, The Session Initiation Protocol (SIP) provides powerful and flexible signaling capabilities for building video conferencing services. Traditionally, for SIP-based centralized video conference systems, the conferencing scale is mainly limited by both the capability of conference server and the availability of bandwidth. In this paper, our design focuses on how to provide dynamic scalability for the SIP-based video conferencing system when the number of conference users increases continually. Based on the study of the SIP protocol and the existing video conferencing models, we propose a dynamic scalable service model that can support to dynamically increase the number of conference servers without negative influence on the stability of system.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

This enables the extra service requests to be transferred and served in the cooperated conference servers. The paper also addresses the SIP-enabled conferencing flows based on the model in detail. We developed a prototype of video conference system based on the proposed model. Experimental results demonstrate the validity of this service model.

Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, In response to the serious scalability and deployment concerns with IP Multicast, we and other researchers have advocated an alternate architecture for supporting group communication applications over the Internet where all multicast functionality is pushed to the edge. We refer to such architecture as End System Multicast. While End System Multicast has several potential advantages, a key concern is the performance penalty associated with such a design. While preliminary simulation results conducted in static environments are promising, they have yet to consider the challenging performance requirements of real world applications in a dynamic and heterogeneous Internet environment. In this paper, we explore how Internet environments and application requirements can influence End System Multicast design.

We explore these issues in the context of audio and video conferencing: an important class of applications with stringent performance requirements. We conduct an extensive evaluation study of schemes for constructing overlay networks on a wide-area test-bed of about twenty hosts distributed around the Internet. Our results demonstrate that it is important to adapt to both latency and bandwidth while constructing overlays optimized for conferencing applications. Further, when relatively simple techniques are incorporated into current self-organizing protocols to enable dynamic adaptation to latency and bandwidth, the performance benefits are significant.

Our results indicate that End System Multicast is a promising architecture for enabling performance-demanding conferencing applications in a dynamic and heterogeneous Internet environment. O. Adeyinka Internet Protocol Security (IPSec) is a standard for securing internet communication and, a widely deployed mechanism for implementing Virtual Private Networks (VPNs). This paper present the performance analysis of IPSec VPNs for videoconference in real time multimedia traffic over a secure communication links by implementing an IPSec-based VPNs technology.

The impact of IPSec VPNs on multimedia under a stress traffic condition with particular attention to transmission delay has been evaluated and the results shows that degradation occurs as IPSec VPNs encrypted with AES could not offer good performance in latency to the video conference.

S Craver, N. Memon, B.L. Yeo, and M.M. Yeung Digital watermarks have been proposed as a means for copyright protection of multimedia data. We address the capability of invisible watermarking schemes to resolve copyright ownership. We show that, in certain applications, rightful ownership cannot be resolved by current watermarking schemes alone. Specifically, we attack existing techniques by providing counterfeit watermarking schemes that can be performed on a watermarked image to allow multiple claims of rightful ownership. In the absence of standardization and specific requirements imposed on watermarking procedures, anyone can claim ownership of any watermarked image. In order to protect against the counterfeiting techniques that we develop, we examine the properties necessary for resolving ownership via invisible watermarking. We introduce and study invertibility and quasi-invertibility of invisible watermarking techniques. We propose noninvertible watermarking schemes, and subsequently give examples of techniques that we believe to be nonquasi-invertible and hence invulnerable against more sophisticated attacks proposed in the paper. The attacks and results presented in the paper, and the remedies proposed, further imply that we have to carefully reevaluate the current approaches and techniques in invisible watermarking of digital images based on application domains, and rethink the promises, applications and implications of such digital means of copyright protection.

III. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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:

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:

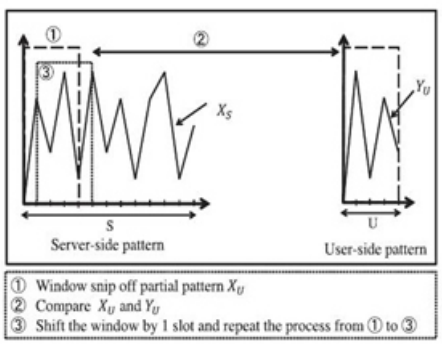

Figure D. Traffic pattern matching.

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.

IV. 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 DPTRAT DPTRAT methods. However, there is no such guarantee in actual network environments.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

V. 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. 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.

VI. Expected result:

Here we are representing diagram to make clear our self with performance variation. Here we are taking two modes i.e. Normal mode and Attack mode. In Normal mode we will get signal waveform and in Attack mode we will get two waveform. This show the variation of proposed method, DP-TRAT and P-TRAT. After seeing diagram we can easily understand the performance variation. Depending upon the variation of video length we will detect our trusted content.

VII. 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 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.

References:

[1]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.
[2]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.
[3]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.
[4]O. Adeyinka, "Analysis of IPSec VPNs Performance in a Multimedia Environment," Proc. Fourth Int'l Conf. Intelligent Environments, pp. 25-30, 2008.
[5]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.
[6]S. Craver, N. Memon, B.L. Yeo, and M.M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications," IEEE J. Selected Areas Comm., vol. 16, no. 4, pp. 573-586, May 1998.
[7]M. Barni and F. Bartolini, "Data Hiding for Fighting Piracy," IEEE Signal Processing Magazine, vol. 21, no. 2, pp. 28-39, Mar. 2004.
[8]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.
[9]E. Diehl and T. Furon, "Watermark: Closing the Analog Hole," Proc. IEEE Int'l Conf. Consumer Electronics, pp. 52-53, 2003.
[10] 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.
[11]Sneha U. Agalawe and Nitin Chopde " A Review on Various Approaches for Detecting and Preventing Content Leakage using Traffic Pattern of Transmission "Computer Science and Engineering Department, SGBAU, India 29 March 2015, Vol.5, No.2 (April 2015).