Volume 2, Issue 11, November-2015, pp. 872-876 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Content Leakage Detection for Trusted Delivery Networks using DRM Technology

[1]LAKSHMANA CHARI, [2] Dr G. RAMA SWAMY

[1](M.Tech) CSE, Dept. of Computer Science and Engineering
[2]Professor, Dept. of Computer Science and Engineering
Priyadarshini Institute of Technology & Science

Abstract: As the rapid development of broadband technologies and the advancement of high-speed networks, 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 protection of the bit stream from unauthorized use, duplication and distribution is the key concern in video streaming services. The conventional Systems addressed this issue by proposing methods based on observation of streamed traffic throughout the network and Digital Rights Management (DRM) is one of the most popular approaches to prevent undesirable contents distribution to unauthorized users. 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. Thus, we enhance the detection performance of the proposed scheme even in an environment subjected to variation in length of video 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: Traffic pattern, Streaming content, leakage detection degree of similarity, multimedia streaming, DRM Technology

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 are 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.

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.

2. LITERATURE SURVEY

In 2014, Hiroki Nishiyama, Desmond Fomo, Zubair Md. Fadlullah and NeiKato,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. RamyaDorai, 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.[2]

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.[3]

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.[4] In 1995, D. Geiger, A. Gupta, L.A. Costa, and J. Vlontzosproposed 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.[5]

III. 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.

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 this 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

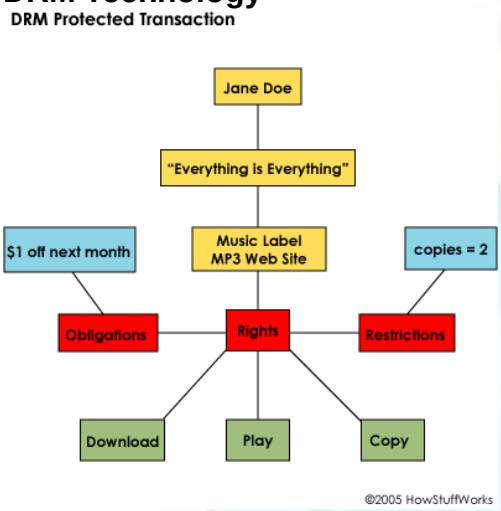
The cross correlation matching algorithm is performed on both the traffic patterns generated through time slot based Algorithm and those generated through packet size based algorithm. The similarity data obtained from the matching of time slot-based generated traffic patterns are considerably small and 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.

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

DRM Technology



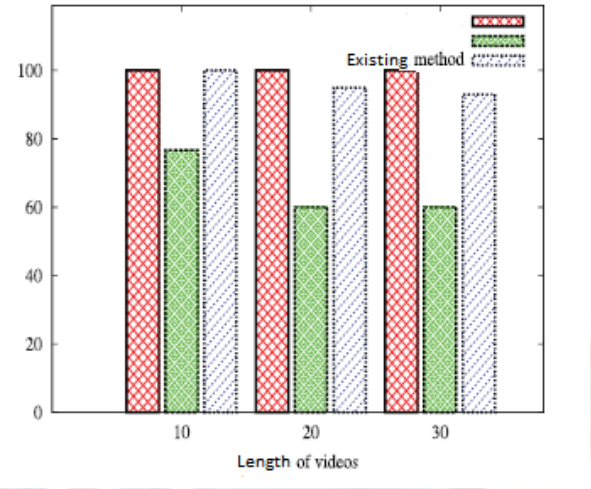
IV PERFORMANCE EVOLUATION

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 Patching algorithm, because DP-TRAT shows high robustness to network environment changes compare to other schemes.

V. EXPERIMENTAL RESULT AND ANALYSIS

This section show the performance analysis of the system and the result gathered from the system works with the Single socket streaming and also with the multi socket streaming. But in proposed system, as it is happening through Multi socket, it takes less time as compared to the existing one. Also its accuracy depends on the throughput, its giving.

COMPARATIVE ANALYSIS OF PROPOSED SYSTEM WITH EXISTING SYSTEM



From the graph 6.3 and 6.4 we can say that the accuracy required for the proposed system is more than the accuracy in existing system with respect to the lengths of different videos. The lengths are in sec. Hence from above comparison we can say that the proposed system is better than the existing one. From the above graph 5 we can see the comparison of existing system and proposed system and we found that the accuracy w.r.t. packet loss in proposed system is more than the existing system. As the streaming is happening through the multi socket the packet are sent from the multi sockets, hence possibility of packet loss is very less. So the accuracy is more in proposed system and again the proposed system is said to be better in accuracy as compared to existing.

VI. 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. And we found that the proposed system is better than the existing system.

REFERENCES

[1] Hiroki Nishiyama, Desmond Fomo, Zubair Md. Fadlullah,, and NeiKato,Fellow," Traffic Pattern-Based Content Leakage Detection for Trusted Content Delivery Networks" IEEE Transaction on Parallel and Distributed System , Volume 25, No 2 Feb 2014
[2] K. Ramya, D. RamyaDorai, Dr. M. Rajaram "Tracing Illegal Redistributors of Streaming Contents using Traffic Patterns" IJCA 2011
[3] S. Amarasing and M. Lertwatechakul, "The Study of Streaming Traffic Behavior," KKU Eng. J., vol. 33, no. 5, pp. 541-553, Sept./Oct. 2006.
[4] M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Traitor Tracing Technology of Streaming Contents Delivery Using Traffic Pattern in Wired/Wireless Environments," Proc. IEEE Global Telecomm. Conf., pp. 1-5, Nov./Dec. 2006.
[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,Aug.
[6] D. Geiger, A. Gupta, L.A. Costa, and J. Vlontzos, "Dynamic Programming for Detecting, Tracking, and Matching Deformable Contours," Proc.IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 17, no. 3, pp. 294-302, Mar. 1995.
[7] R.S. Naini and Y. Wang, "Sequential Traitor Tracing," IEEE Trans. Information Theory, vol. 49, no. 5, pp. 1319-1326, May 2003
[8] O. Adeyinka, "Analysis of IPSec VPNs Performance in a Multimedia Environment," Proc. Fourth Int'l Conf. Intelligent Environments, pp. 25-30,2008
[9] A. Asano, H. Nishiyama, and N. Kato, "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. 1-6, Aug. 2010.

