ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Traffic Pattern-Based Content Leakage Detection

D Naga Lokeswari [1], K Kavya[2], D Madhu Babu[3]

[1]MCA Student, Dept. of MCA, Narayana Engineering College, Nellore, A.P, India

[2] MCA Student, Dept. o MCA, Narayana Engineering College, Nellore, A.P, India

[3]Assistant Professor, Dept. of MCA, Narayana Engineering College, Nellore, A.P, India

ABSTRACT: 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, 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. 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.

KEYWORDS: Streaming content, leakage detection, traffic pattern, packet generation.

I. INTRODUCTION

In recent years the rapid the popularity of real-time video streaming applications and services over the Internet has increased by leaps and bounds. YouTube and Microsoft network video are notable 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 [1], [2], [3] in intra company 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 [4]. A crucial concern in video streaming services is the protection of the bit stream from unauthorized use , duplication and distribution.

Most DRM techniques employ cryptographic or digital watermark techniques [5], [6], [7], [8], [9]. 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 [10]. Hence, streaming traffic may be leaked to P2P networks. In this, we focus on the illegal redistribution of streaming content by an authorized user to external networks. The existing proposals in [12], [13], and [14] monitor information obtained at different nodes in the middle of the streaming path. The generation of traffic pattern does not require any information on the packet header, and therefore preserves the user's privacy. 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. There are five different terms used in this system environment.

1. Leakage detection
2. Traffic pattern matching
3. Cost evaluation
4. Video leakage scenario
5. Streaming traffic

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

II. EXISTING SYSTEM

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 techniques. 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.

III. PROPOSED SYSTEM

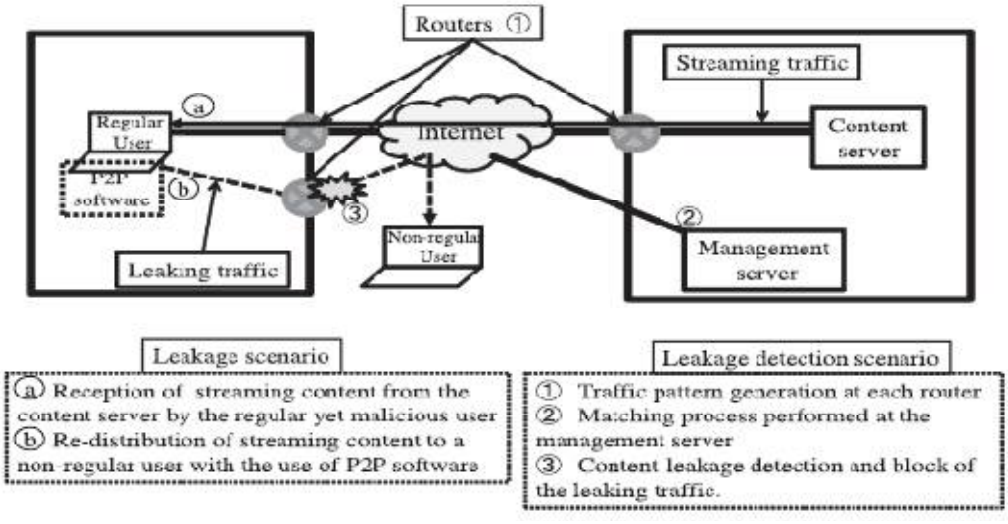
In this paper, we focus on the illegal redistribution of streaming content by an authorized user to external networks. The retrieved information is used to generate traffic patterns which appear as unique waveform per content, just like a fingerprint. The cross-correlation matching algorithm is performed 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 wave-forms is approximated to a normal distribution. On the other hand, the DP matching algorithm is performed on traffic patterns generated through packet size-based algorithm. Therefore, a fixed predefined value is used as the decision threshold. Whether or not patterns are similar is decided by comparing the distance computed through DP matching with the decision threshold, i.e., the distance less than the threshold indicates that the compared traffic patterns are similar.

ADVANTAGES OF PROPOSED SYSTEM:

- ✓ These technologies enhance the distribution of any type of information over the Internet.
- ✓ The traffic pattern generation process performed in conventional methods.

IV. SYSTEM MODELS

The typical content leakage scenario can be described by using the following fig. A regular user in a secure network receives streaming content from a content server. Then, with the use of a P2P streaming software, the regular yet malicious user redistributes the streaming content to a non regular user outside its network.



The matching of time slot-based generated traffic patterns are considerably small and their distribution is considered

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

to be normally distributed around zero, since the distribution of cross-correlation coefficient values of two random wave- forms is approximated to a normal distribution [17]. Therefore, Dobashi [12] use a dynamic decision threshold based on the Chebyshev's inequality, and given by the following equation:

$$\text{© ¼ min}\eth\mu_R \text{ Þ } 4o_R; 1{:}0\text{Þ};$$

Meanwhile, during the matching process of packet size- based generated traffic patterns, the similarity resulting from the comparison of different videos is considerably small, while the similarity resulting from the comparison of similar videos is considerably large. A suitable fixed value is, therefore, used as the decision threshold [12]. To determine whether or not the compared traffic patterns are similar, the maximum value of $RX_U Y_U$ is retrieved and compared to the decision threshold, i.e., $\max\eth RX_U Y_U$ threshold, which indicates that the compared traffic patterns are similar.

On the other hand, the DP matching algorithm is performed on traffic patterns generated through packet size-based algorithm. Therefore, a fixed predefined value is used as the decision threshold [13]. Whether or not patterns are similar is decided by comparing the distance computed through DP matching with the decision threshold, i.e., the distance less than the threshold indicates that the compared traffic patterns are similar.

IV. IMPLEMENTATION

1. MODULES DESCRIPTION

1. Video Leakage setting:

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. First, a regular user in a secure network receives streaming content from a content server. Then, with the use of a P2P streaming software, the regular yet malicious 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.

2. Leakage Detection measures:

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. The topology consists of two main components, namely the traffic pattern generation engine embedded in each router, and the traffic pattern matching engine implemented in the management server. 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 to block leaked traffic.

3. Pattern Generation:

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.

Time slot-based algorithm is a straightforward solution to generate traffic patterns by summing the amount of traffic arrival during a certain period of time, Δt. In case some packets are delayed, they may be stored over the following slot, xi+1, instead of the primary slot, xi. Therefore, delay and jitter of packets distorts the traffic pattern, and as a consequence, decreases the accuracy in pattern matching. Moreover, time slot-based algorithm is affected by packet loss.

Packet size-based algorithm defines a slot as the summation of amount of arrival traffic until the observations 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.

4. Pattern Matching:

In pattern recognition, the degree of similarity is defined to be the similarity measure between patterns. The server-side traffic patterns represent the original traffic pattern. The fundamental method to quantify the similarity of traffic

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

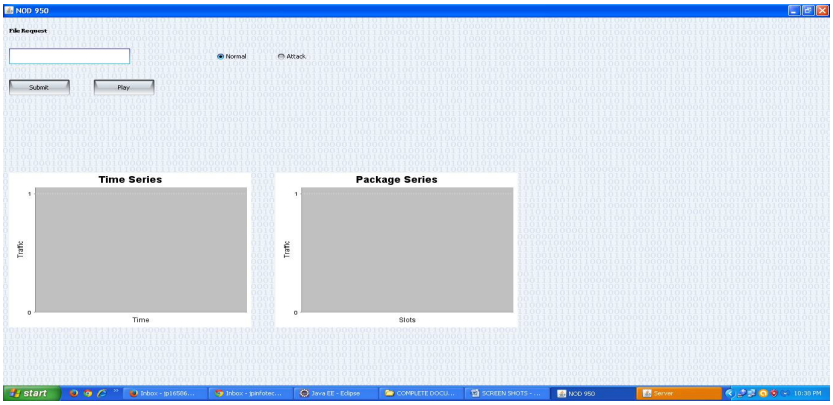
patterns called cross-correlation matching algorithm, consist of computing the cross-correlation coefficient, which is used as a metric of similarity between the various traffic patterns. Before calculating the similarity between the partial pattern XU and the server-side pattern YU.
Another pattern matching algorithm is the dynamic programming (DP) matching based on the DP technique. DP matching utilizes the distance between the compared patterns in U-dimensional vector space as metric representing their similarity.

5. 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 wave-forms is approximated to a normal distribution. On the other hand, the DP matching algorithm is performed on traffic patterns generated through packet size-based algorithm. Therefore, a fixed predefined value is used as the decision threshold. Whether or not patterns are similar is decided by comparing the distance computed through DP matching with the decision threshold, i.e., the distance less than the threshold indicates that the compared traffic patterns are similar.

V. RESULTS AND EXPERIMENTAL STUDIES

Streaming contents are sent from the delivery server to the user, and the traffic is observed at the server side and the user side. Traffic patterns are then generated at the packet observation and sent to the server, where the matching process is performed. To handle variation in network environment such as delay, jitter, and packet loss, we placed the NetEm bridge [23] between the server and the user. P-TRAT- and DP-TRAT- based detection performances are used as comparison to our proposed method.

As an evaluation metric for the performance of the proposed leakage detection method, we define the accu- racy, Pr, and an index of completeness representing the recall ratio, Re [24]. These index are



1.File request generation

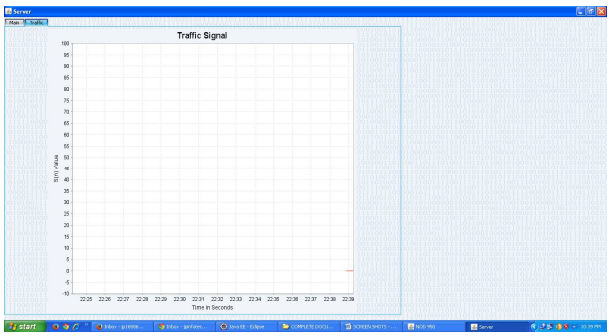
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017



2.Traffic signal generation

3.Leakage detection using attacker

VI. CONCLUSION AND FUTURE WORK

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 o 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

[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] E.D. Zwicky, S. Cooper, and D.B. Chapman, *Building Internet Firewalls*, second ed., O'Reilly and Assoc., 2000.
[12] 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.
[13] K. Matsuda, H. Nakayama, and N. Kato, "A Study on Streaming Video Detection Using Dynamic Traffic Pattern," *IEICE Trans. Comm.*, vol. J19-B, no. 2, pp. 166-176, 2010.
[14] 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.
[15] S. Amarasing and M. Lertwatechakul, "The Study of Streaming Traffic Behavior," *KKU Eng. J.*, vol. 33, no. 5, pp. 541-553, Sept./ Oct. 2006.
[16] Y. Gotoh, K. Suzuki, T. Yoshihisa, H. Taniguchi, and M. Kanazawa, "Evaluation of P2P Streaming Systems for Webcast," *Proc. Sixth Int'l Conf. Digital Information Management*, pp. 343-350, Sept. 2011.
[17] R. Duda, P. Hart, and D. Stock, *Pattern Classification*, second ed.Wiley Interscience, 2000.
[18] 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.
[19] R.S. Naini and Y. Wang, "Sequential Traitor Tracing," *IEEE Trans.Information Theory*, vol. 49, no. 5, pp. 1319-1326, May 2003.
[20] Y. Zhang, P. Ma, and X. Su, "Pattern Recognition Using Interval- Valued Intuitionistic Fuzzy Set and Its Similarity Degree," *Proc. IEEE Int'l Conf. Intelligent Computing and Intelligent Systems*, pp. 361-365, 2009.

BIOGRAPHY

Mr. D.Madhu Babu is an Assistant Professor of MCA at Narayana Engineering College, Nellore, A.P, India. He had done his M.Tech at Satyabhama University, Chennai. He is pursuing PHD at Vikram Simhapuri University ,Nellore,AP.He guided many projects for PG students. His research interests in mobile ad-hoc networks etc.

Ms. D.Naga Lokeswari is a student pursuing MCA at Narayana Engineering College, Nellore, A.P, India. During my final semester project work we prepared this paper for publishing it in an international journal.

Ms. K. Kavya is a student pursuing MCA at Narayana Engineering College, Nellore, A.P, India. During my final semester project work we prepared this paper for publishing it in an international journal.