International Journal of Innovative Technologies
WWW.IJITECH.ORG
ISSN 2321-8665
Vol.03,Issue.02,
June-2015,
Pages:0106-0109

Enhanced Dynamic Leakage Detection Scheme in Content Delivery Networks using Anomaly Software Agent System

B. RAJANI[1], SHAIK FARHEEN[2]
[1]Assistant Professor, Dept of CSE, Priyadarshini College of Engineering and Technology, Nellore, AP, India
[2]PG Scholar, Dept of CSE, Priyadarshini College of Engineering and Technology, Nellore, AP, India.

Abstract: Now a days the multimedia streaming applications and services are becoming more popular. Hence, the problem of trusted video delivery to prevent unwanted content-leakage has, indeed, become critical. While keeping user privacy, conventional systems have identified this problem by recommending methods based on the study of streamed traffic all over the network. These systems keep upgreat detection accuracy while handling with certain traffic deviation in the network, still, their detection performance significantly reduces owing to the major variation lengths of the video. We mainly concentrate on resolving this problem by offering a new content-leakage recognition system that is strong to the differences in video lengths. We identify a relation among the length of videos to be associated and the likeness between the compared videos by comparing videos of various lengths. Thus, we increase the recognition performance of our system even in an environment related to difference in length of video. With a test bed research, the efficiency of our system is assessed in terms of dissimilarity of video length, variation in delay, and loss of packets.

Keywords: Leak Exposure, Streaming Content, Traffic Configuration, Level of Similarity.

I. INTRODUCTION

In recent years, with the rapid development of broadband technologies and the advancement of high-speed wired/ wireless networks, 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 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. 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. 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. 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 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. 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.

II. DETECTING CONTENT LEAKAGE

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. Example for Video Leakage

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 by the following steps as depicted in Fig. 1. 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 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.

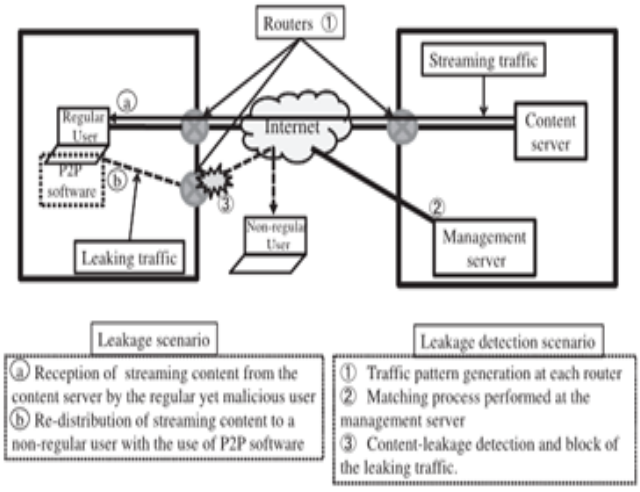

Fig.1. Overview of a leakage scenario and leakage detection scenario.

B. Methods of Leakage Detection

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 in Fig. 1. This 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.

C. Leakage Detection Standard

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. Therefore, Dobashiet al, use a dynamic decision threshold based on the Chebyshev's inequality. 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. To determine whether or not the compared traffic patterns are similar, the maximum value of cross-correlation coefficient is retrieved and compared to the decision 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. 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.

TABLE I: Comparison of Existing Leakage Detection Methods

	Traffic pattern generation algorithm	Traffic pattern matching algorithm	Decision threshold	Robustness
T-TRAT	Time slot-based	Cross-correlation matching	Dynamic (Chebyshev based)	-
P-TRAT	Packet size-based		Static (Fixed value)	Delay and jitter
DP-TRAT		DP matching		Delay, jitter, packet loss

D. Comparison of Current Leakage Detection Methods

The conventional approaches, namely, time slot-based traitor tracing (T-TRAT), packet size-based traitor tracing (P-TRAT), and DP-based traitor tracing (DP-TRAT), based on the aforementioned algorithms are summarized in Table 1. The time slot-based pattern generation algorithm used in T-TRAT is influenced by packet delay and jitter, which deteriorate the user-side traffic pattern. On the other hand, P-TRAT and DPTRAT utilize a traffic pattern generation method based on packet size instead of time slot. As a result, P-TRAT and DPTRAT show robustness against packet delay and jitter. The cross-correlation coefficient is widely use in pattern recognition. However, it is considerably influenced by packet loss that may occur between the streaming server and the user. Meanwhile, DP matching dynamically alleviates this issue, and shows high robustness to variation in network environment such as the occurrence of packet loss. The determination of the predefined decision threshold used in P-TRAT and DP-TRAT is given by computing the median between the degree of similarity resulting from the comparison with the same video and the maximum value of the degree of similarity resulting from the comparison with different videos.

III. IMPROVEMENT OF DETECTION METHOD TO HANDLE VIDEO CONTENTS OF VARIOUS LENGTHS

Among the conventional methods, the 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 DP-TRAT'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 a exponential approximation, and evaluate the computation cost of both the proposed scheme and an eventual enhancement of the previous scheme.

A. Problem Caused by Various Lengths of Videos

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 P-TRAT and DP-TRAT methods. However, there is no such guarantee in actual network environments. Fig. 2 shows an illustration of the occurrence of an erroneous decision in a network environment with different length videos.

B. Proposed System

The proposed scheme is based on computing an approximation curve of the distribution of the pattern size and their associated degree of similarity. Based on the computed curve, we determine the decision threshold specific to each video in our streaming environment. To compute such acurve, we focus on a certain number of pattern sizes less orequal to L.

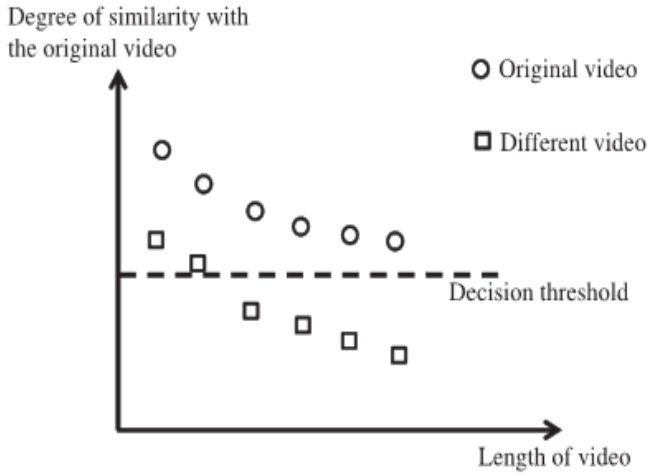

Fig.2.Example of erroneous decision in comparison of different length videos.

The total number of matching is necessary to determine decision threshold specific to each video in our environment. We have to compute the number of matching necessary for the computation of the approximation curve and the number of matching necessary to determine the decision threshold specific to a video, respectively.

IV. PERFORMANCEASSESSMENT

Here, we describe the performance evaluation experiment carried out using a real network environment. We assess the effectiveness and the accuracy of the use of a dynamic decision threshold in a network environment with videos of dissimilar length. Moreover, we calculate the robustness of our system to network environment changes. The proposed decision threshold determination method 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 systems.

A. Testing Configuration for Proposed System

Fig.3 displays the test bed used for the experiment. 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 points as displayed in fig.3, 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 Net Embridge between the server and the user. P-TRAT- and DP-TRAT based detection performances are used as comparison to our proposed method.

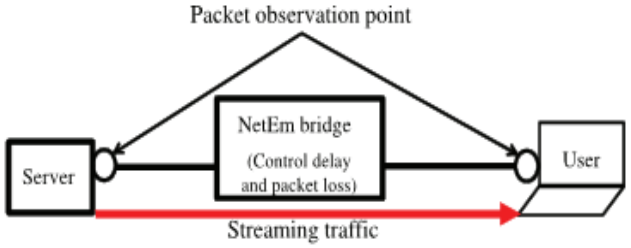

Fig.3. Topology of our conducted experiment.

As an evaluation metric for the performance of the proposed leakage detection method, we define the accuracy, P_r, and an index of completeness representing the recall ratio, R_e. These indexes are widely used in recognition techniques and performance evaluation of web information retrieval systems. P_r and R_e are defined as follow:

$$P_r = C/A \quad (1)$$

$$R_e = C/W \quad (2)$$

where, C, A, and W represent the outflow correctly detected as similar to the original video, the outflow seen as similar to the original, including erroneous judgment, and the outflow of the targeted contents, respectively.

It is worth noting that the bigger the accuracy and the recall ratio, the better the leakage detection performance. However, a tradeoff relation exists between the accuracy and the recall ratio. We consider both and define their harmonic mean F-measure: F. F-measure is given by the following equation:

$$F = (2 \times P_r \times R_e) / (P_r + R_e) \quad (3)$$

B. Performance for Dissimilar Lengths of Videos

In this test, we use a set of different videos having the same length, which can be perfectly distinguished using the conventional methods, P-TRAT and DP-TRAT. From this

set, we generate portions of video of different lengths varying from 30 to 300 seconds. From the generated portions of videos, we randomly choose and send 10, 20, and 30videos from the server to the user. We then observe the amount of traffic, generate the traffic pattern, and perform the matching process. In other word, the performance degradation observed in this experiment can be considered to be caused by the existence of videos with different lengths. P-TRAT and DP-TRAT are used for comparison. With the DP-TRAT, the increase in the number of videos decreases the accuracy. The absence of an adequate method to set the decision threshold handling videos of different length causes the occurrence of erroneous decision in the detection performance of the DP-TRAT. With the conventional methods, the recall ratio is slightly affected by the variation of video lengths. Compare to the conventional methods, the proposed scheme is not affected by the variation of video lengths.

C. Robustness to Network Environment Variations

To evaluate the robustness of the proposed scheme to the variation in network environment, we perform two experiments. Here, we consider a network environment similar to the previous, with 30 videos of lengths varying from 30 to300 seconds. For the first experiment, we generate delay at the Net Em varying from 0 to 200 ms every 25 ms. none of the methods is affected by delay. This is due to the fact that all of these methods generate traffic patterns using the packet size-based generation algorithm, which shows robustness against packet delay jitter. For the second experiment, with the Net Em, we generate packet loss. The generated packet loss rate varies from 0.1 to5 percent. The accuracy in both the conventional methods and the proposed method is not affected by packet loss. For P-TRAT, the recall ratio decreases rapidly when the packet loss exceeds 0.3 percent. Thus, P-TRAT that uses the cross-correlation matching technique, deals ineffectively with variation of traffic amount per slot due to packet loss. We can see that the detection performance of DP-TRAT is slightly affected by packet loss. Meanwhile, our proposed method is not affected by packet loss, and keeps a high detection performance. These two experiments show that the proposed method outperforms the conventional methods. Moreover, it results in high robustness against change in network environment.

V. CONCLUSION

The content leakage recognition system based on the declaration that each streaming content has a distinct traffic pattern is an advanced solution to avoid illegal reallocation of contents by a regular, however malicious user. However, three typical conservative methods, specifically, T-TRAT, P-TRAT, and DP-TRAT, show robustness to delay, jitter or packet loss, the detection performance declines with significant variation of video lengths. We attempt to solve these problems by presenting a dynamic leakage detection system. Additionally, we explore the performance of the proposed technique under an ctual network environment with videos of dissimilar lengths. The proposed system allows flexible and precise streaming content leakage detection independent of the length of the streaming content, which increases secured and trusted content distribution.

VI. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] A. Golaup and H. Aghvami, “ A Multimedia Traffic Modeling Framework for Simulation-Based Performance Evaluation Studies,”Int’l J. Computer and Telecomm. Networking, vol. 50, no. 12, pp. 2071-2087, Aug. 2006.

[5] 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.

[6] M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A.Jamalipour, “Traitor Tracing Technology of Streaming ContentsDelivery Using Traffic Pattern in Wired/Wireless Environments,”Proc. IEEE Global Telecomm. Conf.,pp. 1-5, Nov./Dec. 2006.