Kastala Sandhya* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.3, Issue No.3, April - May 2015, 2193 – 2195.

Maintaining of User Privacy by Managing Reliable Video Delivery

KASTALA SANDHYA
M.Tech Student
Dept of CSE
Malla Reddy Engineering College for Women
Hyderabad, T.S, India

G.PRABHAKAR
Assistant Professor
Dept of CSE
Malla Reddy Engineering College for Women
Hyderabad, T.S, India

Abstract: **Due to the recognition of streaming delivery of movies, expansion of P2P streaming software has concerned much consideration. These technologies improve the allocation of any type of information above Internet. In our work we study on unlawful redistribution of streaming content by means of authorized user towards external networks. Throughout process of video streaming, changes of amount of traffic come out as an exceptional waveform particular to content consequently by monitoring information recovered at various nodes within network, leakage of content can be noticed. In our work we put forward a novel scheme of content-leakage detection that is robust towards variation of video length. The traditional approaches, specifically, time slot-based traitor tracing (T-TRAT) uses algorithm of time slot-based pattern generation and weakens user-side traffic pattern; packet size-based traitor tracing (P-TRAT), along with DP-based traitor tracing (DP-TRAT) makes use of traffic pattern generation technique based on packet size thus, both of them confirms robustness against packet delay as well as jitter.**

Keywords: **Streaming, Content leakage, Packet delay, Video, Jitter.**

I. INTRODUCTION

Real-time communications of video streaming using Internet with virtual private networks (VPNs) were organized widely in a huge number of corporations as a dominant means of promoting business actions devoid of extra costs. An important issue in streaming services of video is the securing of bit stream from illegal use as well as distribution [1]. In our work we study on unlawful redistribution of streaming content by means of authorized user towards external networks. The existing works in literature monitors information that is obtained at several nodes in middle of path concerning streaming. The existence of videos of various lengths within network setting causes a substantial degradation in performance of leakage detection as a result, building up a novel method of leakage detection tough to variation of video lengths is, certainly necessary. One of the most accepted approaches for prevention of objectionable contents that are distributed to illegal users is digital rights management (DRM) expertise. Most of the DRM methods utilize cryptographic or else digital watermark methods on the other hand; these approaches have no important consequence on content redistribution, restored at user-side by approved yet malicious users. Redistribution is strictly no longer complicated by means of peer-to-peer streaming software.

II. OUTLINE OF NETWORK TOPOLOGY CONCERNING LEAKAGE DETECTION

In recent times, with quick expansion of high-speed networks, recognition of applications concerning real-time video streaming services over Internet has improved by leaps and bounds. Due to the recognition of streaming delivery of movies, expansion of P2P streaming software has concerned much consideration [2]. These technologies improve the allocation of any type of information above Internet. A typical content-leakage situation was shown in fig1 in which a regular user within a protected network receives the content of streaming initially from a content server. By P2P streaming software, the yet malevolent user redistributes content of streaming towards a non regular user exterior of its network. Such leakage of content is almost not detected by watermarking or other techniques. Throughout process of video streaming, changes of amount of traffic come out as an exceptional waveform particular to content consequently by monitoring information recovered at various nodes within network, leakage of content can be noticed. In our work we put forward a novel scheme of content-leakage detection that is robust towards variation of video length. An outline of network topology concerning proposed leakage detection system consists of two most important components, specifically traffic pattern generation engine which is embedded in every router, as well as traffic pattern matching engine executed in the management server thus, every router can monitor its traffic volume and produce traffic pattern. Process of traffic pattern generation is based on moreover time slot-based algorithm or else a packet size-based algorithm. Algorithm of Time slot-based is a simple explanation to make traffic patterns by means of summing amount of traffic arrival throughout a convinced period of time. Time slot-

based algorithm is influenced by packet loss. Algorithm of Packet size-based defines a slot as summing up of quantity of arrival traffic until examination of a convinced packet size [3][4]. This algorithm uses packet arrival order as well as packet size, hence is robust to modify in environment. On the other hand, algorithm of packet size-based shows no robustness towards packet loss. In pattern recognition, measure of similarity is defined as similarity measure among patterns. The elemental method to compute resemblance of traffic patterns known as cross-correlation matching algorithm, consist of computing cross-correlation coefficient, which is employed as a metric of resemblance among the variety of traffic patterns [5].

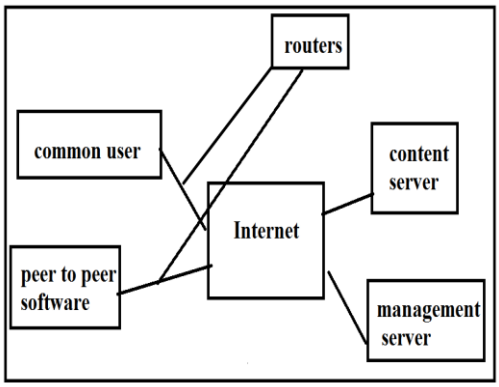

Fig1: Typical content-leakage situation

III. AN OVERVIEW OF PROJECTED SYSTEM

The traditional approaches, specifically, time slot-based traitor tracing (T-TRAT) uses algorithm of time slot-based pattern generation and weakens user-side traffic pattern; packet size-based traitor tracing (P-TRAT), along with DP-based traitor tracing (DP-TRAT) makes use of traffic pattern generation technique based on packet size thus, both of them confirms robustness against packet delay as well as jitter. DP-TRAT technique proves to exhibit high robustness towards packet delay, jitter, as well as packet loss. On the other hand existence of videos concerning various lengths subjected to time disparity in real environment of content delivery causes DP-TRAT's accurateness to reduce. In our work we introduce a novel threshold determination method on basis of an exponential approximation. Traffic patterns concerning streaming videos correspond to skeleton carrying their features and are distinctive for each of the content. Consequently, longer the traffic pattern is additional information on video it displays. In conventional means, it is believed that an assured length of content can constantly be obtained all the way through network for the entire contents. The proposed system is on basis of computing an approximation curve of distribution of pattern size and their connected degree of similarity. On basis of computed curve, the decision threshold was determined for each video which was specific in streaming environment. The total number of matching, essential to find out decision threshold specific to every video in our setting is specified by representing number of matching which are essential for computation of approximation curve as well as number of matching essential to find out decision threshold specific towards a video. The projected decision threshold determination method is put into practice into DP-TRAT which utilizes the packet size-based traffic generation algorithm and as it shows high robustness towards network environment changes when compared to other schemes. In a practical environment, projected scheme attains a lower computation expenditure and it turn out to be much more effectual as number as well as or size of videos enhance [6].

IV. CONCLUSION

In recent times, with quick expansion of high-speed networks, recognition of applications concerning real-time video streaming services over Internet has improved by leaps and bounds. An important issue in streaming services of video is the securing of bit stream from illegal use as well as distribution. The existence of videos of various lengths within network setting causes a substantial degradation in performance of leakage detection as a result, building up a novel method of leakage detection tough to variation of video lengths is, certainly necessary. In our work we study on unlawful redistribution of streaming content by means of authorized user towards external networks. In our work we put forward a novel scheme of content-leakage detection that is robust towards variation of video length. Process of traffic pattern generation is based on moreover time slot-based algorithm or else a packet size-based algorithm. The traditional approaches, specifically, time slot-based traitor tracing (T-TRAT) uses algorithm of time slot-based pattern generation and weakens user-side traffic pattern; packet size-based traitor tracing (P-TRAT), along with DP-based traitor tracing (DP-TRAT) makes use of traffic pattern generation technique based on packet size thus, both of them confirms robustness against packet delay as well as jitter. The projected decision threshold determination method is put into practice into DP-TRAT which utilizes the packet size-based traffic generation algorithm and as it shows high robustness towards network environment changes when compared to other schemes. The proposed system is on basis of computing an approximation curve of distribution of pattern size and their connected degree of similarity.

V. 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.D. Zwicky, S. Cooper, and D.B. Chapman, Building Internet Firewalls, second ed., O'Reilly and Assoc., 2000.

[3] 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.

[4] S. Amarasing and M. Lertwatechakul, "The Study of Streaming Traffic Behavior," KKU Eng. J., vol. 33, no. 5, pp. 541-553, Sept./ Oct. 2006.

[5] 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.

[6] R. Duda, P. Hart, and D. Stock, Pattern Classification, second ed. Wiley Interscience, 2000.

