IJRRECS/June 2015/Volume-3/Issue-6/4131-4135 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

IMPLEMENTATION OF CONSISTENT VIDEO DELIVERY FOR MANAGING USER PRIVACY

Tulala Rani[1], U.Sivaji[2]

[1]M.Tech Student, Department of CSE, St. Martin's Engineering College, Dhulapally (V), R.R (Dist.), T.S, India

[2]Professor, Department of CSE, St. Martin's Engineering College, Dhulapally (V), R.R (Dist.) T.S, India

ABSTRACT:

Because of multimedia streaming services, issue of responsible video delivery to put off intolerable content-leakage has, certainly, developed into critical. A vital issue within video streaming services is defending bit stream from unlawful use, and distribution. While preserving of user confidentiality, conventional systems have proposing methods based on study of streamed traffic all the way through network. Introduction of an innovative leakage detection means tough to variation of video lengths is, definitely essential. We introduce strategy of content-leakage detection that is novel and tough towards variation of video length. In our work we mostly limelight on unlawful redistribution of streaming content by means of authorized user towards external networks. By comparing several length videos, we set up a relationship among length of videos to be compared and their resemblance. Projected leakage detection system contains two main components are specifically traffic pattern generation engine that is embedded in every router, as well as traffic pattern matching engine that is put into practice in management server. We set up a novel threshold determination means on basis of exponential approximation, and consider computation cost of projected scheme. The projected system is on basis of computing an approximation curve of distribution of pattern size as well as their connected degree of resemblance.

Keywords: Content-leakage, Video streaming, Threshold determination, Pattern matching.

1. INTRODUCTION:

In recent times, by rapid advancements of broadband technologies and wireless networks, popularity of synchronized applications of video streaming over Internet has increased [1]. For preventing distribution of objectionable contents to unofficial users to protect authors' copyrights is digital rights management technology which is one of the acceptable methods. However these approaches apply cryptographic or else digital watermark methods and contain no important effect on redistribution of contents by approved yet malicious users. Hence in our work we mainly spotlight on illegal redistribution of streaming content by means of authorized user towards external networks. Expansion of peer to peer streaming software has concerned much attention in recent times which improve distribution of any type of information on Internet. All through video streaming procedure, the changes of amount of traffic come into view as an exceptional waveform particular to content as a result by monitoring recovered information at different nodes within network, detection of content-leakage can be made. We put forward a novel strategy of content-leakage detection that is tough towards variation of video length [2][3]. By means of comparing several length videos, we establish a relationship among length of videos to be compared and their resemblance. In a realistic environment, system achieves a slighter computation cost in assessment to improvement of previous system, and it becomes much more effectual since number and size of videos enhance. Moreover it permits accurate streaming content leakage detection regardless of length of streaming content, which improve protected and trustworthy content delivery. We determine decision threshold facilitating accurate leakage detection still in an environment with several length videos.

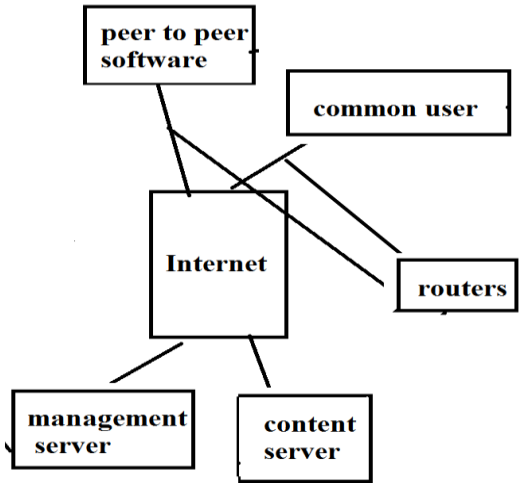

Fig1: An overview of typical content-leakage situation.

2. AN OVERVIEW TOWARDS DISCOVERY OF LEAKED CONTENT:

Due to recognition of multimedia streaming services, the issue of trustworthy video delivery to put off objectionable content-leakage has, certainly, turn out to be critical. Instantaneous video streaming communications by means of virtual private networks are being extensively deployed in a huge number of corporations as a dominant means of promoting business activities without extra expenses.An important concern within video streaming services is protecting bit stream from illegal use, and distribution. While user privacy preservation, traditional systems have proposing methods based on study of streamed traffic all the way through network. These conventional systems preserve high detection accurateness while coping with several traffic variations in network on the other hand; their discovery performance substantially degrades owing to important variation of video lengths [4]. Developing of an innovative leakage detection means tough to variation of video lengths is, certainly necessary. In a leakage situation of content, regular user within a secure network obtain streaming content from a content server and subsequently by usage of peer to peer streaming software, normal yet malicious user reorganize streaming content towards a non-regular user exterior to its network. Such leakage of content is almost not detected by several techniques such as watermarking and digital rights management methods. In the overview of projected leakage detection system two main components are viewed specifically traffic pattern generation engine that is embedded in every router, as well as traffic pattern matching engine that is put into practice in management server. Each router can view its traffic volume and produce traffic pattern for the time being, traffic pattern matching engine figures similarity among traffic patterns all the way through a matching procedure, and based on particular criterion, notices contents leakage. The result is subsequently notified to target edge router to obstruct leaked traffic.

3. ENHANCING OF DETECTION METHOD TOWARDS MANAGING OF VIDEO CONTENTS:

Procedure of traffic pattern generation is on the basis of moreover time slot-based algorithm or else a packet size-based algorithm. Time slot-based algorithm is a simple solution to construct traffic patterns

through summing up of traffic arrival during a certain period. Packet size-based algorithm describes a slot as summation of amount of arrival traffic until examination of a convinced packet size. This algorithm makes usage of packet arrival order as well as packet size, consequently is robust to alter in environment for instance delay and jitter. The cross-correlation matching algorithm is executed on traffic patterns generated all the way through time slot-based algorithm and those produced through packet size-based algorithm. The traditional methods, specifically, time slot-based on traitor tracing (T-TRAT), DP-based on traitor tracing (DP-TRAT) and packet size-based on traitor tracing (P-TRAT). The time slot-based algorithm of pattern generation used in time slot-based on traitor tracing is influenced by packet delay as well as jitter, which get worse user-side traffic prototype. P-TRAT as well as DPTRAT makes the most of a traffic pattern generation system based on packet size rather than time slot. P-TRAT and DPTRAT illustrate robustness against packet delay as well as jitter. The cross-correlation coefficient is extensively utilized in pattern recognition but is significantly influenced by packet loss that may take place between streaming server as well as user [5]. Among traditional methods, DP-TRAT method explains high robustness towards packet delay, jitter, as well as packet loss. The occurrence of videos of separate lengths subjected to time variation in actual content delivery environment cause DP-TRAT's accurateness to reduce. While focussing on DP-TRAT, we set up a novel threshold determination method on basis of exponential approximation, and assess computation cost of projected scheme. The projected scheme is on basis of computing an approximation curve of distribution of pattern size as well as their connected degree of similarity. In a practical environment, our proposed system attains a lower computation outlay in assessment to improvement of earlier method, and it becomes much more effectual since number and or size of videos enhance. In a practical environment, our projected system achieves a lesser computation cost in assessment to improvement of previous system, and it becomes much more effectual since number and size of videos enhance. The projected technique permits flexible and precise streaming content leakage detection regardless of length of streaming content, which improve protected and trustworthy content delivery [6].

4. CONCLUSION:

In recent times, extension of peer to peer streaming software has concerned much attention in recent times which improve distribution of any type of information on Internet. Instant communications of video streaming by virtual private networks are being extensively deployed in a huge number of corporations. The established systems safeguard high detection accuracy while coping with several traffic variations in network on the other hand; their discovery performance substantially degrades owing to important variation of video lengths. Introduction of a pioneering leakage detection means tough to variation of video lengths is, certainly necessary. We put forward a novel strategy of content-leakage detection that is tough towards variation of video length. By comparing quite a lot of length videos, we set up a association between length of videos to be compared and their resemblance. Method of traffic pattern generation is on basis of moreover time slot-based algorithm or else a packet size-based algorithm. Introduced method permits flexible and precise streaming content leakage detection regardless of length of streaming content, which improve protected and trustworthy content delivery.

REFERENCES

[1] O. Adeyinka, "Analysis of IPSec VPNs Performance in a Multimedia Environment," Proc. Fourth Int'l Conf. Intelligent Environments, pp. 25-30, 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] 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.

[4] 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.

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

[6] 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.