IJRRECS/June 2015/Volume-3/Issue-6/4021-4025 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

MAINTENANCE OF BALANCED VIDEO STREAMING FOR DEFENDING USER PRIVACY

Gattu Kranthi Kumar[1], J.V.Krishna[2]

[1]M.Tech Student, Dept of CSE, Holy Mary Institute of Technology & Science, Hyderabad, T.S, India

[2]Associate Professor & HOD, Dept of CSE, Holy Mary Institute of Technology & Science, Hyderabad, T.S, India

ABSTRACT:

Instantaneous communications of video streaming communications by virtual private networks are extensively organized in several corporations as an influential means for promotion of business activities devoid of additional costs. Existence of videos concerning separate length in network environment causes a substantial degradation in leakage detection performance. The approach of content leakage detection which is based on the actuality that each streaming content has a exceptional traffic pattern is a novel solution to put off illegitimate redistribution of contents by a normal, yet malevolent user. We make a focus on prohibited redistribution of streaming content in our work by means of a certified user towards external networks. We commence a new threshold determination means on basis of exponential approximation, and assess computation cost of projected scheme. The projected system is on basis of computing an approximation curve of distribution of pattern size and their associated degree of similarity.

Keywords: Video streaming, Similarity, Virtual private networks, Leakage detection.

1. INTRODUCTION:

To put off unwanted contents distribution towards unauthorized users and protection of author copyrights is digital rights management (DRM) expertise. Most of these techniques make use of cryptographic or else digital watermark methods [1]. In our work we spotlight on prohibited redistribution of streaming content by means of a certified user towards external networks. We commence a novel threshold determination means based on exponential

approximation. In a practical setting, our projected system attains a lower computation outlay in comparison to improvement of earlier schemes, and it turn out to be much more efficient since the number as well as size of videos enhance. A critical issue in video streaming services is fortification of bit stream from illegal use as a result; developing a pioneering leakage detection means robust towards variation of video lengths is, certainly necessary. In our work by means of comparing distinct length videos, we find out a connection among length of videos to be compared and their resemblance. Based on this association, we establish decision threshold enabling precise leakage recognition even in different length videos. The content leakage detection scheme based on the actuality that each streaming content has a exceptional traffic pattern is a novel solution to put off illegitimate redistribution of contents by a normal, yet malevolent user [2][3]. In the typical video leakage situation, as a result of recognition of streaming delivery of movies, improvement of peer to peer streaming software has concerned much consideration. A regular user within a protected network obtains streaming content from a content server and subsequently, with the usage of a peer to peer streaming software, normal yet malevolent user redistributes streaming content towards a non-regular user exterior its network and such content-leakage is almost not detected.

2. AN OVERVIEW OF CONVENTIONAL SCHEMES:

The generation of traffic pattern does not necessitate any information on packet header, and consequently preserves the user's privacy. Leakage discovery is executed by comparing generated traffic patterns. On the other hand, existence of videos of separate length in network environment causes a substantial degradation in leakage detection performance. The traditional approaches, specifically, are time slot basis traitor tracing (T-TRAT), DP-basis traitor tracing (DP-TRAT), and packet size-basis traitor tracing (P-TRAT). The time slot-basis pattern generation algorithm utilized in T-TRAT is influenced by means of packet delay as well as jitter, which worsen user side traffic prototype. DP-basis traitor tracing, and packet size-basis traitor tracing make use of a traffic pattern generation technique on basis of packet size rather than time slot. Hence DP-basis traitor tracing,

and packet size-basis traitor tracing show strength against packet delay as well as jitter. The cross-correlation coefficient is extensively utilized in pattern identification. However, it is noticeably influenced by packet loss that might take place among streaming server as well as user. DP matching energetically lessens issue, and illustrates high toughness towards difference in network environment such as incidence of packet loss. The determination of predefined decision threshold that is utilized in DP-basis traitor tracing, and packet size-basis traitor tracing is represented by computing median among degree of resemblance resulting from comparison with similar video as well as highest value of the degree of resemblance ensuing from assessment with different videos [4].

3. AN OVERVIEW OF PROPOSED SYSTEM:

Right through video streaming process, changes of traffic come into view as a exceptional waveform particular to content. Consequently by scrutinizing information that is retrieved at separate nodes within network, content-leakage can be noticed. An indication of network topology of projected leakage detection system consists of two most important components, specifically traffic pattern generation engine fixed in each router, and traffic pattern corresponding engine executed in management server. Presence of videos of separate length in network environment causes a substantial degradation in leakage detection performance. The projected method is on basis of computing an approximation curve of distribution of pattern size as well as their connected degree of similarity. Each router can watch its traffic volume and produce traffic pattern. For the time being, traffic pattern matching engine work out similarity among traffic patterns all the way through a matching procedure, and based on specific condition, detects contents escape. The result is subsequently notified towards the target edge router to obstruct leaked traffic. Among traditional methods, DP-basis traitor tracing method illustrates high robustness towards packet delay, jitter, as well as packet loss. The existence of videos of separate length subjected towards time variation in actual content delivery setting causes DP-basis traitor tracing, accuracy to diminish. While focussing on DP-basis traitor tracing, we initiate a novel threshold determination means based on exponential

approximation, and assess computation cost of projected scheme. Traffic patterns concerning streaming videos symbolize skeleton carrying their characteristics and are distinctive for content. Consequently, longer traffic pattern is, additional information on the video it exhibits. In established methods, it is supposed that a convinced length of content can constantly be obtained all the way through the network for the entire contents hence; it is likely to make use of a permanent decision threshold in DP-basis traitor tracing and packet size-basis traitor tracing methods. There is no such assurance in authentic network environments [5]. From original video, we generate portions of videos of altering lengths, and we produce their equivalent traffic patterns which are subsequently compared to unique traffic pattern to carry out a sampling of length of videos and their equivalent degree of resemblance. The projected method is on basis of computing an approximation curve of distribution of pattern size as well as their connected degree of similarity. Based on computed curve, we find out decision threshold particular to each video in streaming setting. In a practical environment, our proposed method attains a lower computation outlay in comparison to improvement of earlier schemes, and it turn out to be much more efficient since the number as well as size of videos enhance [6].

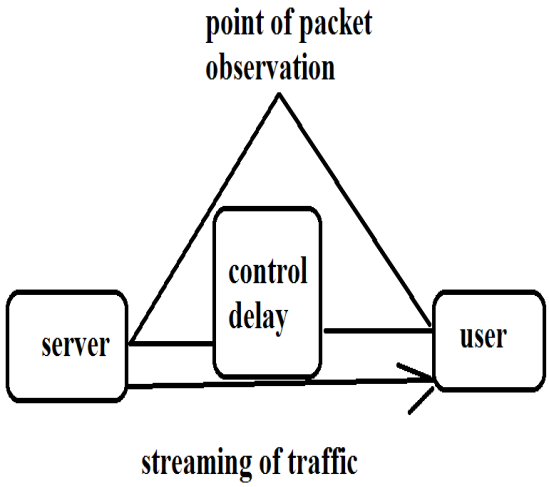

Fig1: An overview of streaming of traffic.

4. CONCLUSION:

In representative video leakage circumstances, due to recognition of streaming delivery of movies, improvement of peer to peer streaming software has concerned much consideration. In our work we draw attention towards prohibited redistribution of streaming content by means of a certified user towards external networks. We start a new threshold determination means based on exponential approximation, and assess computation cost of projected scheme. The conventional approaches, exclusively, are time slot basis traitor tracing, DP-basis traitor tracing, and

packet size-basis traitor tracing. In recognized methods, it is imaginary that a certain length of content can constantly be obtained all the way through the network for the entire contents hence; it is likely to make use of a permanent decision threshold in DP-basis traitor tracing and packet size-basis traitor tracing methods. The introduced method is on basis of computing an approximation curve of distribution of pattern size as well as their connected degree of similarity. In a practical setting, our means attains a lesser computation outlay in comparison to enhancement of earlier schemes, and it turn out to be much more efficient since the number as well as size of videos enhance. DP matching illustrates high robustness towards difference in network environment such as incidence of packet loss. Among conventional methods, DP-basis traitor tracing system illustrates high strength towards packet delay, jitter, as well as packet loss.

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] 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.