ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Robust Content-leakage detection Technique

Umesh Kummari
MTech Student
Department of CSE
Vijaya Krishna Institute of Technology and Sciences
Hyderabad, Telangana.

B.Suman
Associate Professor
Department of CSE
Vijaya Krishna Institute of Technology and Sciences
Hyderabad, Telangana.

ABSTRACT

At this time the popularity of multimedia applications and services are taken top position. Therefore the issue of delivery trusted content becomes very critical i.e. content leakage, content spoofed, illegal redistribution and packet loss. While addressing these issue and providing robust streaming performance by proposing streaming traffic based algorithms and prevent illegal redistribution of content between users to network which has been done by unauthorized users. In this paper we have maintained a high detection accuracy [4] to get content leakage and we areprotecting that to send trusted content to certain destination without outside effect upon content. Due to lack of streaming performance some time, we lose the data. Therefore we have drawn attention over the streaming protocol to propose this issue by using streaming protocols while focusing on streaming traffic in a networks. One of the major issue has been removed by this paper is illegal redistribution by proposing technique do not affect original content.

Keywords- ***Streaming content, redistribution, performance, leakage detection, traffic***

1. Introduction

As we know that technology is being developed one after another to provide better services to user after keeping in mind the drawback of previous version. Because in this era every things are going fast if any of services are not performing their work, those services are being useless. That's why here I am taking an action for increasing proper streaming performance to watch online video. YouTube isone of the notable example of online video streaming [5]. In daily life we are using huge amount of content online like daily news, entertainment related video, music, education concern audio or video. So, we need to provide high level of streaming performance to make easy to get steamed in less speed of internet connection.

While using video streaming we need to care about protection of each streaming bit from unauthorized users, duplication, distribution, etc. Here the mean of copyright is to make duplicate content. To protect this issue we are using technique called digital rights management (DRM). Whenever, this type of approaches are being performed then we need not to worry relevance to protection of content. Due to lack of protection level we get duplication of trusted content as well as misuse. Therefore here we are paying much attention to remove such types of problem or difficulty and enhancetraffic streaming performance with valuable protection.

In this paper, mostly we discus relevance to illegal redistribution of streaming data which is done by an unauthorizeduser[12]. While sending or receiving content there is a chance of content leakage. Here content leakage is nothing but redistribution of content so we need to prevent it. For preventing it we should monitor path to eliminate content leakage and generate traffic pattern [1], [2], [3] for trusted content delivery. Actually we detect leakage of streaming contents for external networks while detecting point from where contents are being leaked. In this proposal technique we are keeping in mind different length of video for comparison then after we draw attention on relationship between the lengths of videos. On behalf of relationship we justify decision threshold to get accurate point of content leakage detection even in

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

network environment with different length videos.

2. Problem Statement

At this time we are facing more problems of streaming content leakage for transferring trusted content. Due to leakage of streaming content, the performance of streaming content become very less and in this case there is chances to lose actual content. On the other hand malicious users are attempting to retrieve our data as well as they also put best effort to spoof our content. Indeed these types of issues happen when contents are being streamed. Some important disadvantages are mentioned below-

No protection for the bit stream is given to prevent unauthorized use, duplication, distribution

Undesirable content distribution is very much possible by unauthorized and Digital Rights management (DRM) is not possible.

In peer to peer(P2P) [8] network streaming [3] traffic may be leaked while redistribution is not technically longer difficult by using P2P [4] steaming software. It is quit tough to entirely protect content leakage using packet filtering alone why because malicious user uses unspecified packet header information therefore they can easily spoof.

An authorized user is very much eligible to use illegal redistribution of streaming content due to it streaming performance is affected.

3. Motivation

In this paper we are proposing robust streaming performance [6] and eliminating illegal redistribution of streaming content and enhance the streaming performance while generating traffic pattern. In middle of streaming path the existing proposals monitor information obtained at different nodes. To generate traffic patterns retrieved information is used to appear unique waveform per content same as a finger print. Indeed there are two techniques by that we can easily generate traffic pattern one is time slot- based algorithm and other one is packet size- based algorithm both are discussed in section 3.1 Some important advantages are mentioned below-
Enhance streaming performance of content with high robustness.

To generate streaming traffic pattern for delivering trusted content while prevent illegal redistribution.

Independently the approximation curve enable accurate comparison of length video. Enhance effectiveness and accuracy to use dynamic decision threshold in network video of different length. Flexible and accurate streaming content leakage detection and increase high security to deliver trusted content.

Pattern Generation Algorithm

Earlier we have discussed about two traffic pattern generation algorithms. Actually for generating traffic pattern it is necessary to use either time slot-based algorithm or packet sized- 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. In case some packets are delayed, they may be stored over the slot, instead of the primary slot. 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 observation of certain packet size. This algorithm only make 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. System Architecture

In this section we are explaining architectureof my paper. Actually it shows regular user and non-regular user to display real time problem with server and how

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

this type of problem has been solved by management sever. After seeing system architecture we can easily understand content leakage.

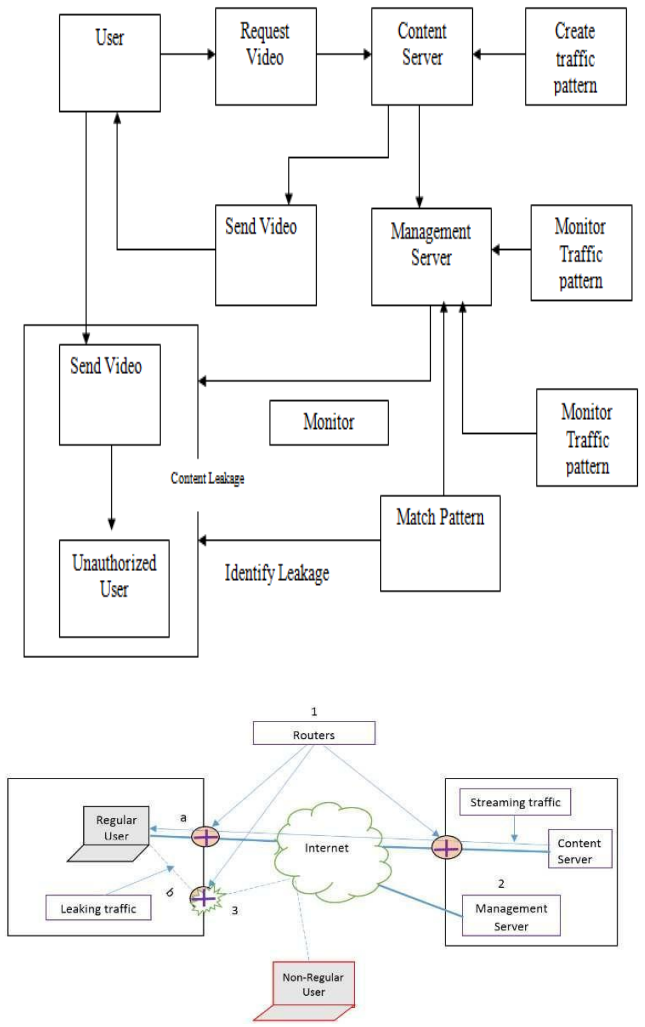

Fig 1.0 System Architecture

In the above figure 1.0 leakage scenario is explained as follows-

The position marked (a) in the above diagram explains reception of streaming content from the content server by the regular user yet malicious user.

The position marked (b) in the above diagram explains Re-distribution of streaming content to a non-regular user with the use of P2P software.

The position marked (1) in the above diagram explains traffic pattern generation at each router.

The position marked (2) in the above diagram explains matching process performed at the management server.

The position marked (3) in the above diagram explains Content-leakage detection and block of the leaking traffic.

In the above proposed architecture we blocking content leakage traffic with the help of management server. Management sever is fully responsible to block such traffic which has been got in way of leaking at the time content streaming. Spoofing of streaming content [5] is mostly done through non-regular user when content distribution is done by regular user. Regular user is nothing but authorized where non-regular user is unauthorized user. Generally the step from where data is distributed to send appropriate place is router.

5. Modules

- Authorized User
- Unauthorized User
- Content server
- Management Server
- Leakage Detection
- Bandwidth requirement

Authorized User

Authorized user requests video of interest file to content server. Content server transmits the video by splitting it into number of small chunks/packets. The chunks are transmitted via router to reach the user. The chunks/packets are aggregated at the user side to get the complete video. Authorized user may some time transfer vide to unauthorized users.

Unauthorized User

Unauthorized users are one, who gets video file redistributed from the authorized user. They are said to be non-regular users or malicious users. A regular user in a secure network receives streaming content from a content server and then redistribute it to the non-regular users.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Content Server

Content server is one, which stores all video content, which servers the regular users upon their request for particular content. The server-side traffic pattern is registered and represents the original traffic pattern. Traffic patterns are then generated at the packet observation points.

Management Server

Management server is one, which monitors the traffic pattern from server side and user side. Time slot base traffic pattern is considered, 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.

Leakage Detection

When the regular user stream video to the non- regular user, it is considered to be content leakage detection. The cross-correlation matching algorithm is performed on the traffic patterns generated through time slot-based algorithm. When there is a variation found, it is detected as content leakage.

Bandwidth Requirement

A minimum bandwidth requirement is need for any node in the network for successful data transmission. We assign a threshold limit for the bandwidth level. The node which receives data or transmits data must meet the minimum requirement level of bandwidth, it should be equal or above the threshold limits. By checking the bandwidth before transmission of data, one can avoid many attacks such as DDOS attacks.

Description of the convention methods

The major approaches of conventional methods are time slot-based traitor tracing(T-TRAT), packet size-based traitor tracing (P-TRAT), and DP based traitor tracing (DP-TART) [9], [10], [11] based on the aforementioned algorithms. Thetime slot based pattern generation algorithm are used in T-TRAT is being influenced by packet delay and jitter, which destroy the user side traffic pattern. Where P-TRAT and DP-TRAT are using a traffic pattern generation method and depend upon packet size in place of time slot. According to result P-TRAT and DP-TRAT[11] display robustness against jitter and packet delay. The cross-correlation coefficient is mostly used in pattern construction. Some timeit is consider as influenced by packet loss which may come between the streaming server and the user. While DP matching dynamically alleviates this type of issue and display much robustness for variation in network environment such as the occurrence of packet loss. The determination of the pre known result threshold used in P-TRAT and DP-TRAT [9], [10]. With computation median between the degree of similar result from the compression with same video and mostly value of the degree of similar result from the compression with different type of video.using a real network environment. We justify the effectiveness and the accuracy of the use of a dynamic decision threshold in a network environmentwith videos of different length. Moreover, we justify the robustness of our scheme to network environment changes. The proposed result threshold determination technique is implemented into the DP-TRAT [9] which employs the packet size-based traffic generation algorithm and the DP-matching algorithm, why because DP TRAT displays high robustness to network environment changes compare to other schemes.

Performance on variation of video length

Here we are representing diagram to make clear our self with performance variation. In below diagram we took nine points and that points showing the variation of proposed method, DP-TRAT and P-TRAT. After seeing diagram we can easily understand the performance variation-

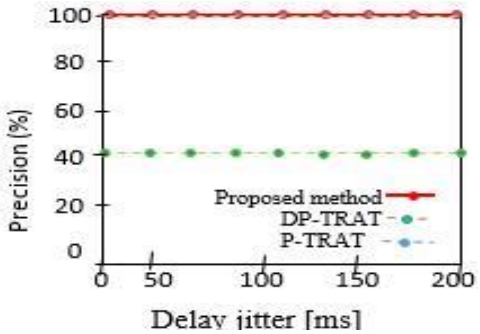

Fig. Accuracy

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

6. Evaluation of performance

Here we discuss about evaluation of performance. This experiment carried out

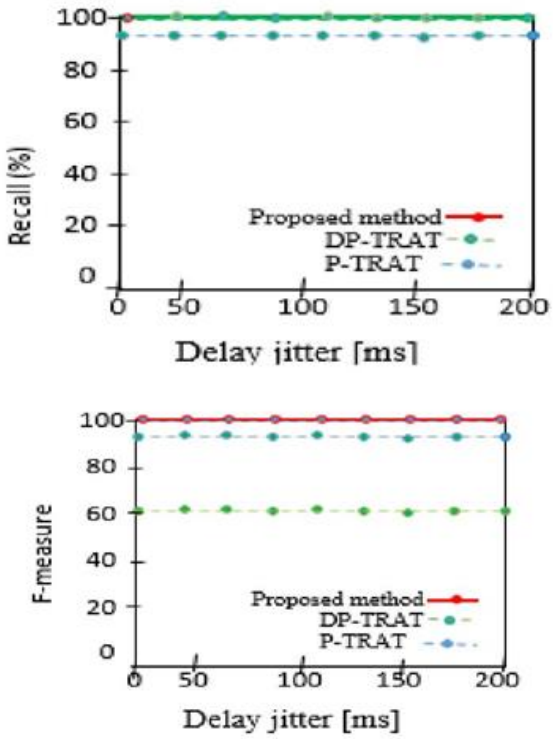

Fig. Recall ratio

7. Conclusion

Enhance streaming performance and protect illegal redistribution is based on the fact that each streaming content has a unique traffic pattern is an innovative solution to protect illegal redistribution of data by a regular user, yet malicious user. Though three typical conventional methods, namely, T-TRAT, P-TRAT, and DP-TRATshow robustness to delay, jitter or packetloss, the detection performance decreases with considerablevariation of video lengths [7]. In this paper efforts to solve these types of issues by introducing a dynamic leakage detection scheme.

Over all this paper is very much suitable to understand streaming performance and protection on streaming content. Illegal redistribution is one of themajor disadvantages of streaming content and here we have successfully solved this problem.

8. References

1.Hiroki Nishiyama, Desmond Fomo, Zubair Md. Fadlullah, and Nei Kato "Traffic Pattern-Based Content Leakage Detection for Trusted Content delivery networks" IEEE Transactions on Parallel And Distributed Systems,Vol. 25,No. 2,February 2014.

2 Content Leakage Detection by Using TrafficPattern for Trusted Content Delivery NetworksVol. 5 (6) , 7909-Research on the Traffic Behavior Characteristics ofP2P Streaming MediaISSN 2079-8407Vol. 4, No. 1 Jan 2013.

4.K. Matsuda, H. Nakayama, and N. Kato, "A Study on StreamingVideo Detection using Dynamic Traffic Pattern," IEICETransactions on Communications (Japanese Edition), vol.J19-B,no.02, 2010.

5.Z. Yang, H. Ma, and J. Zhang, "A Dynamic Scalable Service Modelfor SIP-Based Video Conference," Proc. Ninth Int'l Conf. ComputerSupported Cooperative Work in DE, pp. 594-599, May 2005.

6.O. Adeyinka, "Analysis of IPSec VPNs Performance in a MultimediaEnvironment," Proc. Fourth Int'l Conf. Intelligent Environments,pp. 25-30, 2008.

[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.

[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.