ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

An Approach for Detecting and Preventing Content Leakage Using Traffic Pattern of Transmission

Sneha U.Agalawe[1], Prof. Nitin R. Chopde[2]

PG Student, Department of Computer Science & Engineering, SGBAU, India[1]

Assistant Professor, Department of Computer Science & Engineering, SGBAU, India[2]

ABSTRACT: As the rapid development of broadband technologies and the advancement of high-speed networks,the video streaming applications and service's popularity over the Internet has increased. The protection of the bit stream from unauthorized use, duplication and distribution is the key concern in video streaming services. Digital Rights Management (DRM) is one of the most popular approaches to prevent undesirable contents distribution to unauthorized users but it have no significant effect on redistribution of contents, decrypted or at the user-side by authorized yet malicious users and content leakage. Also preserving user privacy, conventional systems have addressed this issue by proposed methods based on the observation of streamed traffic throughout the network. These conventional systems maintain high detection accuracy while coping with some of the traffic variation in the network. However, the detection performance considerably degrades due to the significant variation of video lengths. This work proposes a content-leakage detection scheme that is robust to the variation of the video length. By comparing videos of different lengths, a relation between the length of videos to be compared and the similarity between the compared videos is determined. Therefore, the detection performance of the proposed scheme even in an environment subjected to variation in length of video will enhance. The effectiveness of proposed scheme is evaluated in terms of variation of video length, delay variation, and packet loss. Also, increased in bandwidth, which enhance the performance of transmission, include a module to enhance the performance of overall system.

KEYWORDS: content-leakage, Traffic pattern

I. INTRODUCTION

In recent years, with the rapid advance in broadband technology, digital contents delivery applications have been used widely. The streaming technology has made the contents delivery more popular. Due to the increasing popularity of multimedia streaming applications and services, the issue of trusted video delivery to prevent undesirable content-leakage has, indeed, become critical .The popularity of real-time video streaming applications and services over the Internet has increased by leaps and bounds. 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 is served, by using streaming transmission technologies. Also, with virtual private networks (VPNs), real-time video streaming communications such as web conference in intra company networks or via Internet are being widely deployed in a large number of corporations as a powerful means of efficiently promoting business activities without additional costs.Rather than packet filtering by firewall-equipped way out nodes is an easy solution to avoid leakage of streaming contents to external networks. In this solution, the packet header information that is 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 .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**.** The existing proposals monitor information obtained at different nodes in the middle of the streaming path. The retrieved information are 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

performed by comparing the generated traffic patterns. In this paper, the focus is on the illegal redistribution of streaming content by an authorized user to external networks.

II. LITERATURE SURVEY

In 2014, Hiroki Nishiyama, Desmond Fomo, Zubair Md. Fadlullah and NeiKato,Fellow proposed a paper on "Traffic Pattern-Based Content Leakage Detection for Trusted Content Delivery Networks". There is no requirement of any information on the packet header in the generation of traffic pattern, and therefore preserves the user's privacy. The detection of leakage is then performed by comparing the generated traffic patterns. However,in the leakage detection performance, the existence of videos of different length in the network environment causes a considerable degradation. Hence,by comparing different length videos, developing an innovative leakage detection method robust to the variation of video lengths is indeed required.

In 2011 ,K. Ramya, D. RamyaDorai, Dr. M. Rajaram proposed paper on "Tracing Illegal Redistributors of Streaming Contents using Traffic Patterns" .The packet size-based traffic pattern generatoradaptation, instead of the time slot based one used in T-TRAT, enables P-TRAT to accomplish robustness to packet delay jitter. The DP matching employment as a pattern matching technique permits DP-TRAT to remove the effect of packet losses. In addition, with significant results on the relations between such algorithms, and the robustness to packet reordering and encryption provides us by their work. However, the important concern in adopting both time slots based and packet size-based traffic generators consisted in the issue of packet reordering, which may have a substantial impact upon the performances of all the conventional methods.[2]

In 2006 ,S. Amarasing and M. Lertwatechakul proposed a paper on "The Study of Streaming Traffic Behavior," KKU Eng. J., vol. 33, no. 5, pp. 541-553. The understanding of streaming traffic behavior is still advantageous for network system development to capably support streaming traffic in the future. To observe the different traffic behaviors of on-demand traffic (stored-media traffic) and real-time live trafficis the main objective. Moreover, also the study of the relation between encoding bit rates and streaming traffic behavior is carried out.[3]

In 2006 M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, proposed paper "Traitor Tracing Technology of Streaming Contents Delivery Using Traffic Pattern in Wired/Wireless Environments," propose a system to detect illegal contents streaming by using only traffic patterns which are assembled from the amount of traffic traversing routers. They also investigate a way to cope with random errors and burst errors which occur regularly in wireless environment and show the agreeable result which they have obtained in a practical testing environment.[4]

In 1995, D. Geiger, A. Gupta, L.A. Costa, and J. Vlontzosproposed a paper on "Dynamic Programming for Detecting, Tracking, and Matching Deformable Contours" Particular this approach as applied to medical images, the main field of applications considered, was first considered in. The formulation of the cost functions has been subjective by their work. Minimizing an energy function is a typical way to identify deformable shapes. A constraint of this approach has been that the algorithms are slow, iterative, and not guaranteed to discover the global minimum. Moreover, they argue that some of the user input data has not been utilized by previous methods.[5]

III. PROBLEM STATEMENT AND DISCUSSION

In existing system,the illegal redistribution of streaming content by an authorized user to external networks is focused. The existing proposals display information obtained at different nodes in the middle of the streaming path. The retrieved information are used to create traffic patterns which appear as unique waveform per content , just like a fingerprint. Any information on the packet header is not required for the generation of traffic pattern, and therefore preserves the user's privacy. Leakage detection is then achieved by comparing the generated traffic patterns. However, the presence of videos of different length in the network environment causes a substantial degradation in the leakage detection performance. Thus, developing an innovative leakage detection method stout to the variation of video lengths is, indeed required.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

IV. DESCRIPTION OF THE PROPOSED WORK

Streaming contents are sent from the delivery server to the user, and the traffic is witnessed at the server side and the user side. Traffic patterns are then created at the packet observation points and sent to the server, where the matching procedure is performed. To handle variation in network environment such as delay, jitter, and packet loss, we placed the bridge in the middle of the server and the user. P-TRAT- and DP-TRAT based detection performances are used as comparison to our proposed method. These indexes are widely used in recognition techniques and performance calculation of web information retrieval systems. It is worth noting that the larger the accuracy and the recall ratio, the better the leakage detection performance. However, a tradeoff relation exists between the exactness and the recall ratio. We consider both and define their harmonic mean F-measure .The organization of the system is as follows: A typical video leakage scenario, detection system and procedures are described. Then, first we illustrate the drawback of the existing scheme due to the variation of video length in realistic environment, then we termed the proposed leakage detection scheme, and we evaluate its calculation cost in judgment to that of the existing scheme. Furthermore, we evaluate the usefulness and the accuracy of the proposed scheme with respect to different length videos, and its robustness to network environment changes.

Proposed Work can be divided into following modules:

- Collection of Video Data set.
- Development of traffic pattern extraction based on the data contained in video.
- Development of server to handle multiple sized video and video fingerprints based on user.
- Development of client for user login and fetching of video from server.
- Modification in server and client to support multi socket based communication for improved bandwidth.
- Request of video by client to server, and recognition of traffic pattern at server, and prevention of content leakage through the fingerprint saved in module3.
- Result evaluation and optimization of system to find delay, throughput, size in video distribution.

V. MODULES DESCRIPTION

1. Collection of Video Data set :

In this module, I collected a set of Videos which will be streamed by the client. This set of videos will be stored on the Server side. Whenever any request for any of the available videos will come, the Server will serve the video after authorization of the Client.

2. Development of traffic pattern extraction based on the data contained in video:

Any video has its attributes such as its Size in Kilobytes, its Length in Seconds etc. So proposed to create a traffic pattern which will be based on the information regarding specific video.

3. Development of server to handle multiple sized video and video fingerprint based on user :

In this module, practically a Server will be created which will serve to the Client's requests. By means of Traffic pattern, each of the video in the Video Data Set will be uniquely identified by the characteristic components of the video.

4. Development of client for user login and fetching of video list from server :

After creation of the Server, any number of Clients can be created. The clients will have to login to the Server. After that, each of the Clients will be able to fetch the available video list contained in Video Data Set.

5. Modification in server and client to support multi socket based communication for improved bandwidth :

In further modification in Server and Client, it will use the multiple sockets. This will result in improvement of the bandwidth. In typical Client-Server communication, the Server has a socket which is bound to a specific port number. But here it will use multiple sockets to improve the bandwidth.

6. Request of video by client to server, and recognition of traffic pattern at server, and prevention of content leakage through the fingerprint saved in module 3. :

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

In this module, Client will request for any of the video from Video Data Set. Server will recognize the traffic pattern of the requested video. We have the fingerprint of each of the video, so matching the requested fingerprint, the Server will feed the video to the Client.

7. Result evaluation and optimization of system to find delay, throughput, and size of video distribution :

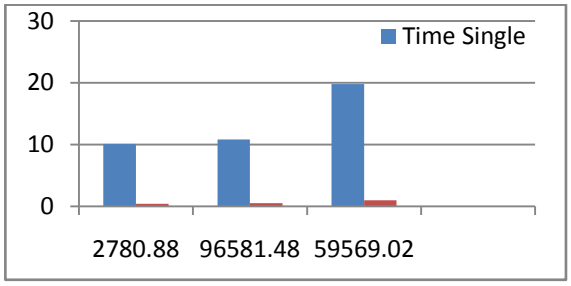
In this last module, the result of the streaming is evaluated. Also the Output and throughput of the distribution of video is calculated.

V. EXPERIMENTAL RESULT AND ANALYSIS

This section show the performance analysis of the system and the result gatherd from the the system works with the single socket streaming and also with the multi socket streaming. But in proposed system, as it is happening through multi socket, it takes less time as compared to the existing one. Also its accuracy depends on the throughput, its giving.

	Size	Time (Single socket) ms	Time (Multi socket) ms
Video 1	2780.88	10.12	0.40
Video 2	96581.48	10.83	0.54
Video 3	59569.02	39.81	0.97

Table 1: Comparison between time required for transmission in single and multi socket streaming



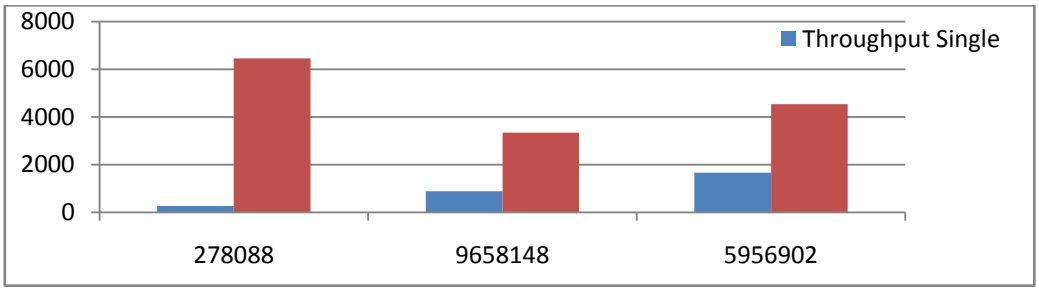
Graph1: Graph of proposed system fortime required w.r.t. different lengths of videos

Graph 1 represent the Graph of the proposed system For time required w.r.t.different lenghts of videos. Here we can see that the time required for the multi socket system is less than time required in multi socket system. That means if comminication happens through the multi socket system then it will be fast commincation than the single socket system.

	Size	Throughput(Single socket)kbps	Throughput (Multi socket)kbps
Video 1	278088	274	6451.678
Video 2	9658148	891	3345.77
Video 3	5956902	1658	4538.3467

Table 2: Comparison between Throughput of transmission in single and multi socket streaming.

The table 2 represent the value obtained for the throughput in single streaming and in multi streaming system.The Throughput can be given as the Length of video by time required to be transmit.



Graph2: Graph of proposed system for throughput w.r.t. different lengths of videos

The figure 2 represents the throughput w.r.t different lengths if videos. As time required for transmission in multi socket system is less ,the throughput will be more As compared to the single socket streaming.

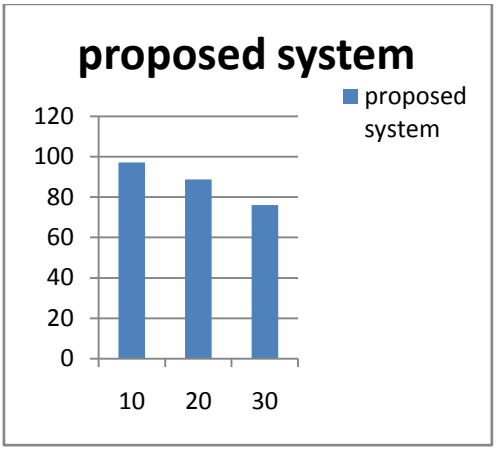
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

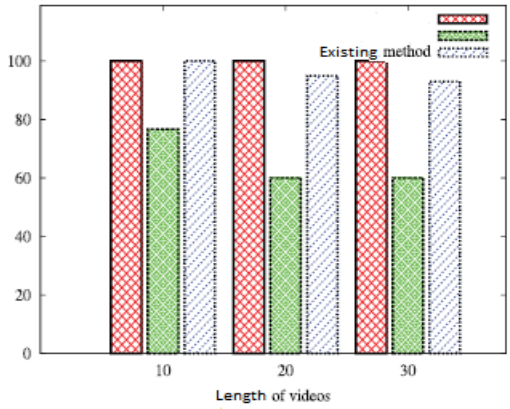
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

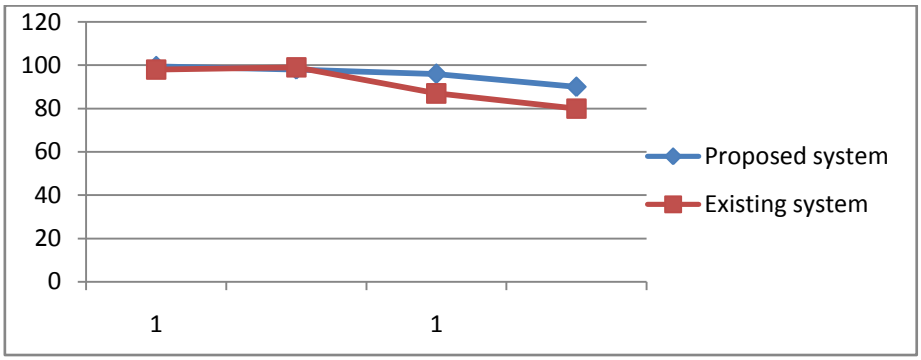
VI. COMPARATIVE ANALYSIS OF PROPOSED SYSTEM WITH EXISTING SYSTEM





Graph 3 and4: Graph for the comparison of proposed system and existing system for accuracy w.r.t.different lengths of videos[1].

From the graph 6.3 and 6.4 we can say that the accuracy required for the proposed system is more than the accuracy in existing system with respect to the lengths of different videos. The lengths are in sec. Hence from above comparison we can say that the proposed system is better than the existing one.



Graph 5: Graph of comparison between proposed system and existing system for Accuracy w.r.t Packet loss.

From the above graph 5 we can see the comparison of existing system and proposed system and we found that the accuracy w.r.t. packet loss in proposed system is more than the existing system. As the streaming is happening through the multi socket the packet are sent from the multi sockets, hence possibility of packet loss is very less. So the accuracy is more in proposed system and again the proposed system is said to be better in accuracy as compared to existing.

VII. CONCLUSIONS

The content leakage detection system based on the fact that each streaming content has a inimitable traffic pattern is an innovative solution to prevent illegal redistribution of contents by a regular, yet malevolent user. Though three typical conventional methods, show robustness to delay, jitter or packet loss, the detection performance drops with considerable variation of video lengths. This system tries to solve these issues by introducing a dynamic leakage detection scheme. Moreover, we investigate the performance of the proposed method under a network environment with videos of different lengths. The proposed method allows malleable and accurate streaming content leakage

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

detection independent of the length of the streaming content, which enhances secured and trusted content delivery. And also use the conception of bandwidth enhancement for the better performance.And we found that the proposed system is better than the existing system.

REFERENCES

[1] Hiroki Nishiyama, Desmond Fomo, Zubair Md. Fadlullah,, and NeiKato,Fellow," Traffic Pattern-Based Content Leakage Detection for Trusted Content Delivery Networks" IEEE Transaction on Parallel and Distributed System , Volume 25, No 2 Feb 2014
[2] K. Ramya, D. RamyaDorai, Dr. M. Rajaram "Tracing Illegal Redistributors of Streaming Contents using Traffic Patterns" IJCA 2011
[3] S. Amarasing and M. Lertwatechakul, "The Study of Streaming Traffic Behavior," KKU Eng. J., vol. 33, no. 5, pp. 541-553, Sept./Oct. 2006.
[4] 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.
[5] Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, "Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture," Proc. ACM SIGCOMM, pp. 55-67,Aug.
[6] D. Geiger, A. Gupta, L.A. Costa, and J. Vlontzos, "Dynamic Programming for Detecting, Tracking, and Matching Deformable Contours," Proc. IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 17, no. 3, pp. 294-302, Mar. 1995.
[7] R.S. Naini and Y. Wang, "Sequential Traitor Tracing," IEEE Trans. Information Theory, vol. 49, no. 5, pp. 1319-1326, May 2003
[8] O. Adeyinka, "Analysis of IPSec VPNs Performance in a Multimedia Environment," Proc. Fourth Int'l Conf. Intelligent Environments, pp. 25-30, 2008
[9] 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.