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

Traffic Delineate-Based Content Outflow Revealing for Trusted Satisfied Delivery Networks

Juttiga Praveen
M.Tech Student,
Department CSE,
D.N.R. College of Engineering & Technology.

DDD.Suri Babu
HOD & Associate Professor,
Department CSE,
D.N.R. College of Engineering & Technology.

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 [1], 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 betterservices 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 datawhich is done by an unauthorizeduser[12]. While sending or receivingcontent there is a chance of content leakage.

Herecontent 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 network environment with different length videos.

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

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 fingerprint.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 enables 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 trafficpattern 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 casesome 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 makes 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 architecture of my paper. Actually it shows regular user and non-regular user to display real time problem with server and how this type of problem has been solved by management sever. After seeing system architecture we can easily understand content leakage.

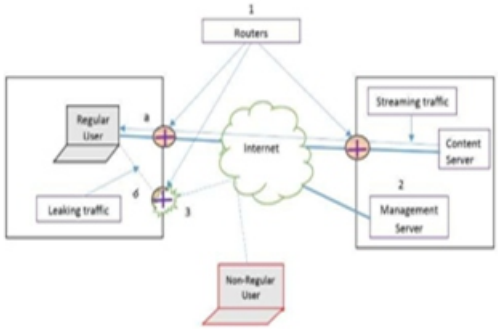

Fig 1.0 System Architecture

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.

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

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.

The following are the modules :
1.Video Leakage setting
2.Leakage Detection measures
3.Pattern Generation
4.Pattern Matching
5.Leakage Detection Criterion

Video Leakage setting:

Due to the popularity of streaming delivery of movies, development of P2P streaming software has attracted much attention. These technologies enhance the distribution of any type of information over the Internet. First, a regular user in a secure network receives streaming content from a content server. Then, with the use of a P2P streaming software, the regular yet malicious user redistributes the streaming content to a non regular user outside its network. Such content-leakage is hardly detected or blocked by watermarking and DRM-based techniques.

Leakage Detection measures:

Throughout the video streaming process, the changes of the amount of traffic appear as a unique waveform specific to the content. Thus by monitoring this information retrieved at different nodes in the network, content-leakage can be detected. The topology consists of two main components, namely the traffic pattern generation engine embedded in each router, and the traffic pattern matching engine implemented in the management server. Therefore, each router can observe its traffic volume and generate traffic pattern. Meanwhile, the traffic pattern matching engine computes the similarity between traffic patterns through a matching process, and based on specific criterion, detects contents leakage. The result is then notified to the target edge router to block leaked traffic.

Pattern Generation:

We describe the traffic pattern generation process performed in conventional methods. Traffic pattern generation process is based on a either time slot-based algorithm or a packet size-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, Δt. In case some packets are delayed, they may be stored over the following slot, x_{i+1}, instead of the primary slot, x_i. 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.

Pattern Matching:

In pattern recognition, the degree of similarity is defined to be the similarity measure between patterns. The server-side traffic patterns represent the original traffic pattern. The fundamental method to quantify the similarity of traffic patterns called cross-correlation matching algorithm, consist of computing the cross-correlation coefficient, which is used as a metric of similarity between the various traffic patterns. Before calculating the similarity between the partial pattern XU and the server-side pattern YU.Another pattern matching algorithm is the dynamic programming (DP) matching based on the DP technique. DP matching utilizes the distance between the compared patterns in U-dimensional vector space as metric representing their similarity.

Leakage Detection Criterion:

The cross-correlation matching algorithm is performed on both the traffic patterns generated through time slot-based algorithm and those generated through packet size-based algorithm. The similarity data obtained from the matching of time slot-based generated traffic patterns are considerably small and their distribution is considered to be normally distributed around zero, since the distribution of cross-correlation coefficient values of two random waveforms is approximated to a normal distribution.

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

On the other hand, the DP matching algorithm is performed on traffic patterns generated through packet size-based algorithm. Therefore, a fixed predefined value is used as the decision threshold. Whether or not patterns are similar is decided by comparing the distance computed through DP matching with the decision threshold, i.e., the distance less than the threshold indicates that the compared traffic patterns are similar.By using Pattern generation algorithm,the packet when lost shows us where the packet is lost .If we want to retransmit the packet that is lost we have to continue with the yes option ,then the graph starts representing the video srtreaming.If we say no the streaming gets stopped there itself. 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.

Traffic Pattern:

Traffic Pattern In animated contents (MPEG), the bit rate is automatically adjusted to the changes of the scene. Each content is considered to have its own characteristic feature just like fingerprint, therefore, the unique information of these contents appear in waveforms. This paper focuses on VBR traffic, which is typical type, used in contents delivery and calls these waveforms “Traffic pattern”. Here, the each content is distributed independently of each streaming server. The traffic pattern is generated by dividing traffic into some chunks of IP packets by following a division policy. There are three division policies 1) Time slot- based Traitor Tracing (T-TRAT) 2) Packet size- based Traitor Tracing (P-TRAT) 3) DP (Dynamic Programming) matched Traitor Tracing (DP-TRAT) The division policy is unique to each conventional method.

In TTRAT, a chunk is composed of packets arriving during the same timeslot. On the other hand, packets, size of which is below a certain threshold, are used as delimiters to determine chunks in both P-TRAT and DP-TRAT approaches. The division policy does not depend on time. Therefore, it is robust against the packets delay. Traffic pattern is defined as amount of traffic for one time slot, a certain period of time Δ t(s) and expressed for N dimension in the following expression. X=(x1,x2,x3,. . . ,xN) t , T = N(Δt) (1) Here, T(s) is the whole length of traffic pattern. Similarity of traffic patterns between certain user side (YU) and a part of server-side pattern XU and use a cross-correlation coefficient as a criterion to judge the similarity of traffic patterns. Calculate the cross-correlation coefficient RXY using the following equation (2). RXY = (X' U) t Y ' U (2) √||X' U ||2 . ||X' U||2 Where −1 < RXY < 1 and X ' U,Y' U are the normalized traffic patterns when the mean = 0, and variance = 1. RXY ’s value would be near to 1, if two vectors were similar to each other.

Comparison of Traffic Pattern Figure:

Overviews the traffic pattern matching process. Since the server-side traffic pattern, XS , and edge router-side traffic pattern, YU, have different lengths in general, i.e., U ≤ S, we employ a sliding window-based method. The size of the window is set to be equal to the length of the receiver side router pattern, U. The pattern matching procedure is repeatedly called(S − U + 1) S M R1 R2 Internet R3 R4 U1 U2 IJCA Special Issue on “Computational Science - New Dimensions & Perspectives” NCCSE, 2011 83 times for different combinations of the edge router-side pattern and a piece of the server-side pattern, XU, clipped from the original pattern, XS , by the sliding window. If and only if even one of the matching results shows that the compared patterns are similar, we may conclude that there is a content leakage. The similarity criteria are different among conventional methods according to the adopted pattern matching algorithm. As described next, the cross-correlation matching coefficient is used in both T-TRAT and P-TRAT approaches. On the other hand, Dynamic Programming (DP) matching is employed in DP-TRAT. Next, the Transform Process in Figure.4 is conducted to prevent influences of burst errors in wireless environment. In the Transform Process, first, vector’s elements whose values are equal or less than a certain threshold TP are removed from the User-side pattern YU (U-dimension) and new User-side pattern YU (U - dimension) are constructed.

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

For example, three elements are removed in Figure 4. Next, the same part of the Server-side pattern's elements as the User-side pattern is also removed and new Server-side pattern XU (U-dimension) is constructed. In Figure 3, three corresponding elements are removed. After the Transform Process, cross correlation coefficient RXY is calculated with Equation (2). After these, sliding the window from left to right is done by one slot and the whole server-side pattern is scanned. We repeat the extraction of pattern XU (U-dimension) from server-side pattern XS (S-dimension), the Transform Process and also calculate the cross-correlation coefficient. Error Losses elements as the User-side pattern is also removed and new Server-side pattern XU (U - dimension) is constructed. In Figure 4, three corresponding elements are removed.

After the Transform Process, cross correlation coefficient RXY is calculated with Equation. After these, sliding the window from left to right is done by one slot and the whole server-side pattern is scanned. We repeat the extraction of pattern XU (U-dimension) from server-side pattern XU (S-dimension), the Transform Process and also calculate the cross-correlation coefficient. If whole server-side pattern XS had S-dimension and user-side pattern YU had Udimension, the number of the calculation would be S-U+1 time. If a large value exists in cross-correlation coefficient graph, it means that a certain user-side pattern is similar to the part of the server-side pattern and such a pattern is called a "matched pattern". In this case, the user is considered to be receiving contents. Figure. 3. Traffic Pattern matching Mechanisms.

4.1 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. Thecross-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 degrees 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.

5.1 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-

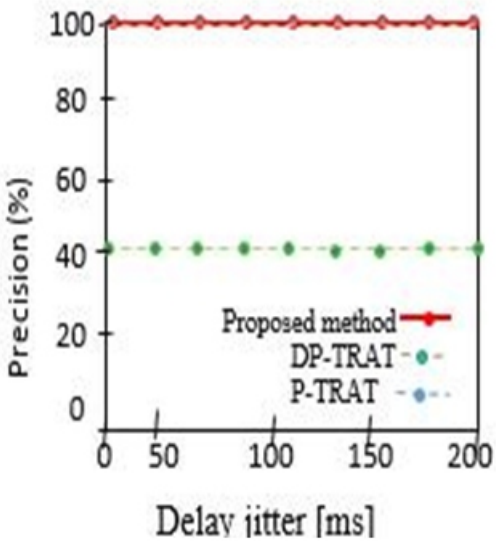

Fig. 5.1.1 Accuracy

5. Evaluation of performance:

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

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

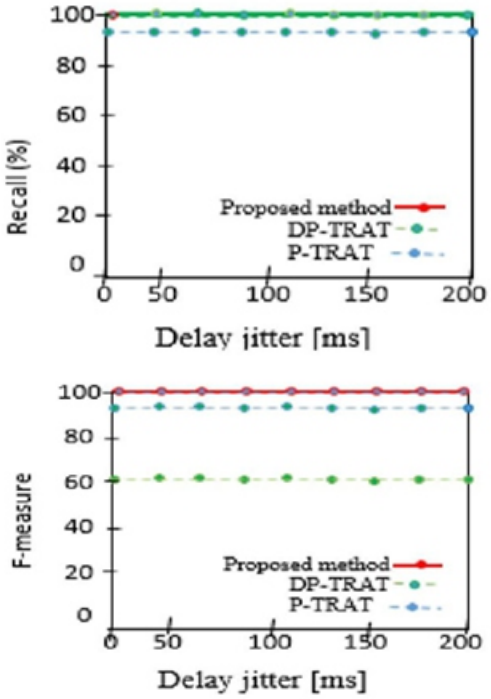

Fig. 5.1.2 Recall ratio

6. 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.

7. References:

1.HirokiNishiyama, 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.

3.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.

4.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.

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