A Payable Secured Monitoring System for Video Streaming and Detecting Content Leakage in Trusted Networks

[1]K.BhavanaPriya, [2]M.Azhagiri
[1]Student, [2]Assistant Professor,
Kingston Engineering College, Vellore

***Abstract*—The data transferred between the source and destination is to build communication and share information. Information can be in any form (text, audio, video, image etc). In this project the multimedia data transferred are in the form of videos. Everything on internet are in the form of packets. A strategy of pattern matching has been utilized to monitor the source and destination content for its originality based on the water marking security concepts. The monitoring system has been designed with leakage analyzer for checking the intrusion or leakage of packets between the transfers of source to destination. A security based packet tracing has been designed and the performance of the monitoring system has been visualized graphically. The leakage of video that is redistribution of videos by the authorized users can be prevented by comparing different length videos, the relationship between the length of videos to be compared and their similarities. Based on this the threshold is determined to find accurate leakage. Everything is done within the trusted networks approved by the profiler.**

IndexTerms—Watermarking,Trusted networks

I. INTRODUCTION

The network security monitor provides the content leakage detection method for the content that are transferred in the trusted network . The content can be data like text, image, audio, video and this method focus on video content. The watermarking technique which is collusion resistant is used for providing the authentication signatures for the content sent in the trusted network. For the leakage detection the novel content leakage detection method that includes the pattern generation and pattern matching algorithms are used. The video streaming may buffer in congestion rich network to avoid buffering the cache to store the streaming video is implemented.

The illegal redistribution of streaming content by an authorized user to external networks is avoided The existing proposals monitor information obtained at different nodes in the middle of the streaming path. The retrieved information is 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 it preserves the user's privacy. Leakage detection is then performed by comparing the generated traffic patterns.

The existence of videos of different length in the network environment causes a considerable degradation in the leakage detection performance. Developing an innovative leakage detection method robust to the variation of video length is required. By comparing different length videos a relationship between the length of videos to be compared and their similarity is determined. Based on this relationship, the decision threshold enabling accurate leakage detection even in an environment with different length videos is determined.

The conventional systems maintain a high detection accuracy while coping with some of the traffic variation in the network (e.g., network delay and packet loss). Their detection performance substantially degrades owing to the significant variation of video lengths. A novel content-leakage detection scheme that is robust to the variation of the video length is proposed to overcome the degradation by comparing videos of different lengths, a relation between the length of videos to be compared and the similarity between the compared videos are generated. Therefore, the detection performance of the proposed scheme even in an environment subjected to variation in length of video is enhanced. Through a test bed experiment, the effectiveness of our proposed scheme is evaluated in terms of variation of video length, delay variation and packet loss.

Sender is an administrator, who sends the content with watermarking information. To enhance the process, a monitoring system is used to detect the content leakage and intrusion .Once monitored the content leakage and intrusion in an application that is transferred as packet there is retransmission until no intrusion or defect in content. It checks the originality of the content after packet transferred from a monitoring system not only the original content also with watermarked content. Monitoring system analyze the originality of the content and it is time consuming while transferring packets. These contents along with watermarked source send to the receiver through monitored system only.

Initially the inputs from the user will be fetched and stored in the database for the standard for sending the data's from the source to the destination. The sender will be sending the packets of data's of information. Every data from the source is sent via packets to reach the destination of the receiver. The loss of packets will be checked and evaluated based on the sent data's of packets transfer. If the data's are lost during packet transfer then obviously , there will be an intruder changing the content in the data packets. Information has been leaked or changed by the intruder or because of any other reasons will be checked in the

information leakage check module. In information leakage check module, packets will be checked on the traversal of source to destination of the specified users accordingly

The packet Monitoring will be emphasized with the checking up of the data loss during the packet transfer from the sender side to the client side data exchange (Real time example of our project is "Video streaming of Data " (YouTube buffering delay concepts). The overall performance of our system will be checked and evaluated in the performance evaluation module based on the original packet data transfer from the user to the receiver of the traffic network scenario.

In addition to the web monitor for leakage detection and analysis of the video streaming without allowing the approved users to redistribute the video content outside the trusted networks the watermarking technique along with the video content to embed the signature of the sender or the secret information to the approved users of the trusted network. In addition to this payment features to this can also be added and to improve the performance of the video streaming analysis can be improved.

Sender is an administrator, who sends the content with watermarking information. To enhance the process, a monitoring system is used to detect the content leakage and intrusion .Once monitored the content leakage and intrusion in an application that is transferred as packet there is retransmission until no intrusion or defect in content. It checks the originality of the content after packet transferred from a monitoring system not only the original content also with watermarked content. Monitoring system analyze the originality of the content and it is time consuming while transferring packets. These contents along with watermarked source send to the receiver through monitored system only.

Online payment for the registration will be typical to implement in web monitoring system within the trusted networks hence the DD number taken by the user to be approved can be entered in case of paid users. The concept of paid users are implemented because the free users may not be reliable. In case of the organisation usage the free users are considered.

- **II SYSTEM ARCHITECTURE**

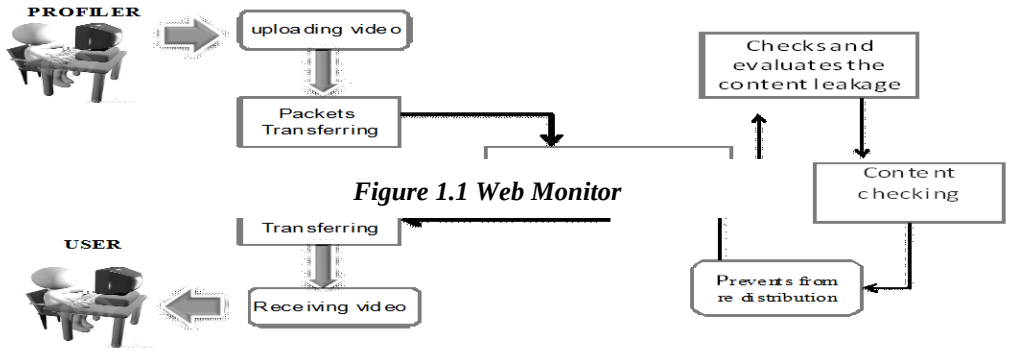


Figure 1.1 Web Monitor

WEB MONITOR

The functional systems used to implement the web monitor are:

1. User Detail
2. Packet Sharing
3. Information Leakage
4. Packet Monitoring
5. Performance Evaluation

2.1 USER DETAIL MODULE

In the user details module, the inputs from the user to register to view the videos will be fetched and stored in the database for approving the user by the standard profiler for allowing the user to see the up loaded files. If the user has the login id and password, he logs in directly if not registers by giving all his credentials. The profiler approves the user and the approval message is sent to the email address that has been registered.

Initially the profiler page is created. The features of the profiler will be

- Approving the registered user.
- Uploading the video file and choosing the definition of the video file.
- Uploading the image by browsing from the system.
- The monitoring system can be switched on.

The user first registers by filling the register form of new users. The genuine details about the users like Name, User id, Password(to be set),Email Id, chosen type of user, etc.

The data message which is a video file is created and the message is split in to packets then for each message packet unique patterns are generated with reference to their packet size else patterns are generated according to time slot.

XN → Sender side pattern profile

YN → Receiver or approved user side

2.2. PACKET SHARING

The data to be shared that is the video file that has to be shared will be split into packets. A packet id will be assigned for each packet that is split. The Video uploaded should be lesser than 4000KB.The packet id is also known as the patterns.

Packet Generation

Packet sharing includes the process of generating the packet (the data) the video file to be sent is split into number of packets.

For each packet the pattern is generated. The pattern for the packets are generated using T_TRAT and P_TRAT. T_TRAT is a time slot based generator. This generates by summarizing the amount of traffic arrival during a certain period of time Δt. P_TRAT is a packet slot based generator. It defines the summation of amount of arrival traffic until the observation of certain packet size.

Pattern Generation Algorithm

Initially the message is generated and split into packets. After splitting the message into packets a pattern is generated based on packet size else the pattern is generated according to time slot

The patterns are generated at both sender and receiver terminals. Later the monitoring system compares both the patterns which are generated. The patterns are generated using the pattern generation algorithm.

2.3. INFORMATION LEAKAGE CHECK MODULE

Information has been leaked or changed by the intruder or because of any other reasons will be checked in the information leakage check module .In this module, packets will be checked on the traversal of source to destination of the specified users accordingly.

The loss of packets will be checked and evaluated based on the sent data's of packets transfer. If the data's are lost during packet transfer then obviously there will be an intruder changing the content in the data packets.

Pattern matching:

Packet size-based algorithm is used for checking originality of the data after transferring packets of data information.

Dp_TRAT Algorithm:

- A pattern generated both sides will be compared.
- Pattern generated on sender side is Xn
- Pattern generated on receiver side is Yn
- Xu and Yu are calculated by taking average and subtracting from each one .
- After calculating Xu , Yu compare both .
- If Xu and Yu are proportional
- Then there is no leakage is detected
- Else
- There is a loss of data

Thus the patterns generated both sides will be matched and the loss rate is evaluated by comparing the patterns of the packets transferred.

Dp-TRAT is an dynamic programming traitor tracing algorithm in which the comparison of two generated patterns are done.

The pattern generated on sender side is Xn and the pattern generated on receiver side is Yn, considering Xn and Yn the values for Xu and Yu are calculated by taking average and subtracting from each one. After calculating Xu and Yu they are compared.

If the Xu and Yu are propositional there it implies that the leakage has not occurred else there is leakage.

2.4. PACKET MONITORING MODULE

The packet Monitoring Module will be emphasized with the checking up of the data loss during the packet transfer from the sender side to the client side data exchange (Real time example of our project is "Video streaming of Data ", i.e. (YouTube buffering delay concepts).

The entire transactions that have been made by the system will be monitored by the monitor. The time of transaction, the size of the video file, the protocol used for the transfer of data and the duration of the video file is logged in the monitoring system.

Monitoring System is the key element that is used to keep track of packets transferring. As soon as the admin/profiler authenticates and initialises the system the traffic monitor is started. Then the Traffic monitor starts initializing and keeps record of point of event system procedure, initial end point and duration of traffic.

2.5. PEFORMANCE EVALUATION MODULE

The overall performance of our system will be checked and evaluated in the performance evaluation module based on the original packet data transfer from the user to the receiver of the traffic network scenario.

Thus the four modules are implemented individually according to the data flow mentioned and the product is developed. The performance evaluation is done after analysing the videos of different lengths. The video analysis is done with different length video and the packet with loss user details , intrusion detection methods and the web monitoring is implemented individually

III. RESULTS AND DISSCUSSION

The robustness of the proposed scheme to the variation in network environment is evaluated and two experiments are performed. Here, a network environment similar to the content leakage method is considered, with 30 videos of lengths varying from 30 to 300 seconds.

For the first experiment, the delay at the NetEm varying from 0 to 200 ms every 25 ms is generated. None of the methods is affected by delay and due to the fact that all these methods generate traffic patterns using the packet size-based generation algorithm, which shows robustness against packet delay jitter.

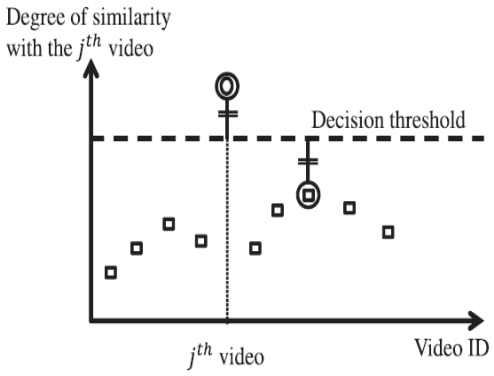
For the second experiment, with the NetEm, packet loss is generated. The generated packet loss rate varies from 0.1 to 5 percent. The accuracy in both the conventional methods and the proposed method is not affected by packet loss. In the P-TRAT, the recall ratio decreases rapidly when the packet loss exceeds 0.3 percent. Thus, P-TRAT that uses the cross- correlation matching technique, deals ineffectively with variation of traffic amount per slot due to packet loss.

The detection performance of DP-TRAT is slightly affected by packet loss. The proposed method is not affected by packet loss and keeps a high detection performance.

P-TRAT and DP-TRAT two experiments show that the proposed method performs the conventional methods. Moreover, it results in high robustness against change in network environment.

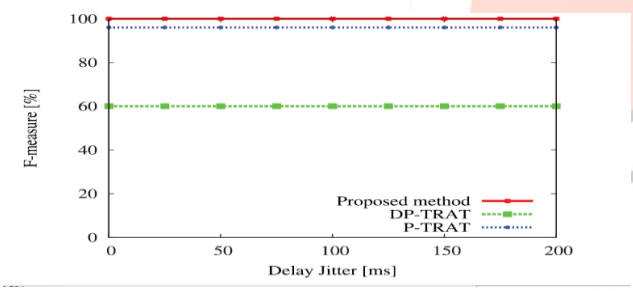
3.1. VIDEO ANALYSIS

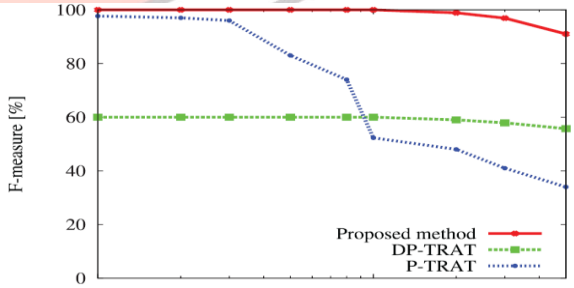
The decision threshold from the original video, we create portions of videos of varying lengths and we generate their corresponding traffic patterns. These patterns are then compared to the original traffic pattern to perform a sampling of the length of videos and their corresponding degree of similarity. With the distribution of the sampling result.The robustness of the proposed scheme to the variation in network environment is evaluated and two experiments are performed. A network environment similar to the previous is considered, with 30 videos of lengths varying from 30 to 300 seconds.



Performance On Delay Of Packets:

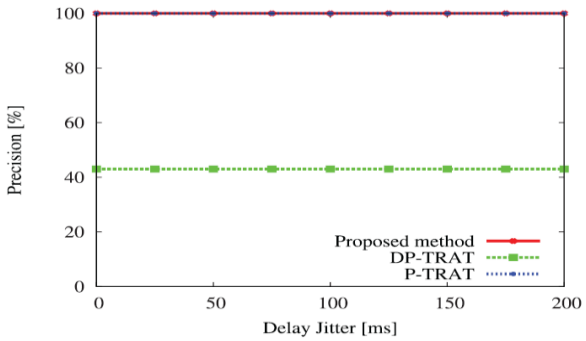
The delay at the NetEm varying from 0 to 200 ms every 25 ms is generated. None of the methods is affected by delay. This is due to the fact that all of these methods generate traffic patterns using the packet size-based generation algorithm, which shows robsustness against packet delay jitter.

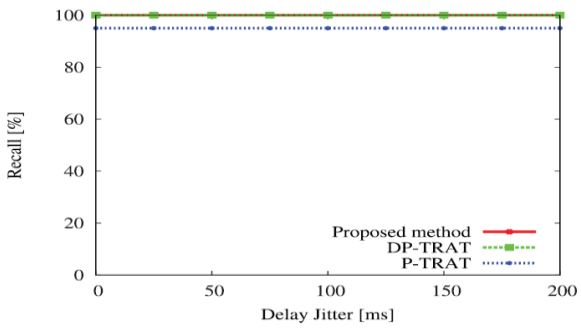




Performance On Packet Loss.

NetEm, packet loss is generated. The generated packet loss rate varies from 0.1 to 5 percent. The accuracy in both the conventional methods and the proposed method is not affected by packet loss. P-TRAT, the recall ratio decreases rapidly when the packet loss exceeds 0.3 percent.





- **IV. CONCLUSION**

The content leakage detection system based on the fact that each streaming content has a unique traffic pattern is an innovative solution to prevent illegal redistribution of contents by a regular malicious user. Though three typical conventional methods , T-TRAT, P-TRAT and DP-TRAT shows robustness to delay, jitter or packet loss .The detection performance decreases with considerable variation of video lengths. Monitor system attempts to solve these issues by introducing a dynamic leakage detection scheme. The performance of the proposed method under a real network environment with videos of different lengths is investigated. The proposed method allows flexible and accurate streaming content leakage detection independent of the length of the streaming content, which enhances secured and trusted content delivery.

- **REFERENCES**

[1]. Chan-il woo1 and seung-dae lee2 (2013) international journal of smart home vol.7, no.5, pp.115-124, http://dx.doi.org/10.14257/ijsh.2013.7.5.12 issn: 1975-4094 ijsh "Digital Watermarking For Image Tamper Detection Using Block-Wise Technique"

[2]. David X. Wei Cheng Jin Steven H. Low Sanjay Hegde in(Dec 2006).in IEEE/ACM Transactions on Networking, Volume. 14, Issue no. 6, pp no.59,"FAST TCP: Motivation, Architecture, Algorithms, Performance."

[3]. Derek Kulinski,Jeff Burke, Lixia Zhang,(July 2013) In IEEE COMSOC MMTC E-Letter Vol.8, No.4, "Video Streaming Over Named Data Networking"

[4]. Dorin comaniciu, senior, visvanathan ramesh and peter meer, (may 2003) ieee transactions on pattern analysis and machine intelligence, vol. 25, no. 5, "Kernel-Based Object Tracking"

[5]. Design,donald graji,mohnish pabrai,uday pahrainovcmber (1990) communications magazine0 163-6804/90/0011-0052 "Methodology For Network Security"

[6]. David watson, matthew smart, g. Robert malan and farnam jahanian,(april 2004) ieee/acm transactions on networking, vol. 12, no. 2, 261, "Protocol Scrubbing: Network Security Through Transparent Flow Modification"

[7]. Ibrahim Alsonosi Nasir, Ahmed b. Abdurrman (, July 3 - 5, 2013) in Proceedings of the World Congress on Engineering 2013 Vol III, issued a paper "A Robust Color Image Watermarking Scheme Based On Image Normalization"

[8]. Kais khaldi and abdel-ouahab boudraa,(march 2013) ieee transactions on audio, speech and language processing, vol. 21, no. 3, 675 "Audio Watermarking Via Emd"

[9]. Mahesh Balakrishnan, Tudor Marian, Kenneth P. Birman, , Hakim Weather spoon and Lakshmi Ganesh (JUNE 2011) IEEE/ACM Transactions On Networking, Volume. 19, Issue no. 617 pp no. 3, "Maelstrom: Transparent Error Correction For Communication Between Data Centers"

[10]. M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto and A. Jamalipour,(Nov./Dec 2006) in Proc. IEEE Global Telecommunications Conference, pp.1-5, San Francisco, USA, "Traitor Tracing Technology Of Streaming Contents Delivery Using Traffic Pattern In sWired/Wireless Environments" which explains Traitor

[11]Mauro barni and franco bartolini , (may 2009), ieee signal processing magazine 1053-5888, "Data Hidind For Fighting Piracy"

[12]. M. Koubaa, C. Ben Amar Regim H. Nicolas Labri(2006) in Proceedings of the Eighth IEEE International Symposium on Multimedia (ISM'06) "Collusion-Resistant Video Watermarking based on video mosaicing"

[13]. R. S. Naini and Y. Wang, in (May 2003), IEEE Trans. Inf. Theory, vol.49, , pp.1319-1326, no.5 proposed a system called "Sequential Traitor Tracing"

[14] Radu O. Preda1, Dragos N. Vizireanu2(sep 2007) IEEE TELSIKS1-4244-1468-7/07. "Blind Watermarking Capacity Analysis Of MPEG2 Coded Video"

[15]. Raghavendra , KChetan K.R (2009) IEEE 978-1-4244-4793-0, Vol 09 "A Blind And Robust sWatermarking Scheme With Scrambled Watermark For Video Authentication"