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. 2, Issue 3, March 2014

Secure Guaranteed Rate Scheduling Of Streams Using Traitor Tracing Technique

R. Kalpana[1] , K.Lalithambigai[2]

[1]Department of Computer Science & Engineering, Pondicherry Engineering College, Pondicherry, India.

[2]Department of Computer Science & Engineering, Pondicherry Engineering College, Pondicherry, India.

ABSTRACT: Today, streaming technology is applied to many applications as it delivers audio and video without making the viewer wait tediously to download files. But a problem that exists in streaming technology is the use of content without knowledge of the content holders and content providers. The digital rights management system protects the rights associated with the use of digital content through various techniques and one among them is Traitor Tracing Systems. General traitor tracing systems uses digital watermarks and encryption keys to ensure content protection. But these techniques are not effective when illegal processes are carried out at the user-side. Another traitor tracing method provides content protection by monitoring traffic patterns constructed from routers. But a 2% delay jitter rate starts to render the video stream unusable and hence monitoring the content becomes a problem. In the proposed scheme a Guaranteed Rate scheduling algorithm is utilized to minimize the delay jitter and to ensure secure delivery of the streaming content. Finally, the results of simulation are provided to demonstrate the effectiveness of the proposed scheme.

KEYWORDS: Digital rights management (DRM); broadcast; streaming contents; traffic pattern; traitor tracing; low-jitter; switch scheduling.

I. INTRODUCTION

Broadband is often called "high-speed" access to the Internet and with its advance the streaming technology is applied to various applications. The goal of streaming media is to work around the bandwidth limitations of the Internet. One of the major pitfalls in streaming technology is that, the content can be pirated by unauthorized access. In order to overcome such piracy issues The Digital Right Management system provides various control techniques to limit the use of digital content. In the existing DRM architectures, the cryptographic techniques are used for secure delivery of the content and the watermarking techniques are used to prove the ownership rights associated with the content.

In the case of cryptography technique, the content providers encrypt the content using encryption keys and securely transmit the encrypted content to the users. Users can then extract the original content using decryption keys, which are provided to users through any key exchange mechanisms. Partial encryption of compressed images and videos is presented in (H. Cheng et al., 2000) and Selective encryption of wavelet packet encoded image data is discussed in (A. Pommer et al., 2003). However, such techniques are not able to restrain distributions of decrypted content or use of plagiarized keys. In case of watermarking technique, an individual identity such as a watermark is assigned to the content (W. Trappe et al., 2003; D. Boneh et al., 1998). However, these method requires a large amount of computations and hence critical for real-time streaming and it is presented in (R. S. Naini et al., 2003). In addition to the computation, there are also known attacks that might tamper the embedded watermark in the content which is presented in (K. Su et al., 2005; M. Barni et al., 2004).

One way to improve the success rate of tracking traitors is to narrow the list of users who may be traitors, by monitoring the content distribution from content providers to the users. The monitoring process should be implemented based on the information obtained at routers in order to prevent user’s interruption and moreover the process does not make use of information inside the packets hence it does not cause any privacy issues (B. N. Park et al., 2005). During the streaming process the traffic pattern is observed at the routers near the content provider and the users. The traffic patterns are then compared to determine whether a user is watching the respective content or not (M. Dobashi et al., 2006; Hidehisa Nakayama et al., 2010).

However, there are many technical challenges to be resolved such as delay, jitter, packet loss rates etc in the above mentioned traitor tracing system and the importance of minimizing the delay jitter is presented in (S. Chand et al., 2007). Even low amounts of jitter or packet loss starts to render the video stream unusable and hence monitoring the content becomes a problem. While streaming the content to many users' two criteria becomes necessary to minimize the above challenges, the first is to reserve resources such as buffer space in each IP router and the second is to use a dynamic switch scheduling algorithm on each IP router to schedule the delivery of the content. In order to minimize the delay jitter while streaming the content, the Guaranteed Rate scheduling algorithm (Ted H. Szymanski et al., 2009) is used and by doing so the determination accuracy of the above mentioned traitor tracing system is also improved.

The rest of this paper is organized as follows. In Section II, an overview of the DRM technology and various traitor tracing systems are introduced. Section III describes some prior guaranteed-rate scheduling algorithms. Section IV describes about the monitoring process of the traitor tracing system. Section V describes the low-jitter scheduling algorithm. Section VI presents the results of simulations with Network Simulator 2. Finally, Section VI concludes the paper.

II. RELATED WORK

This section of the paper discuss about various existing traitor tracing techniques to attain the DRM's primary objective. The use of digital video provides opportunities for anyone to make illegal copies and distributed them easily. The digital rights management (DRM) systems play a vital role to preserve the economic value of digital video and protect the rights of the owners (F. Hartung et al., 2000; R. H. Koenen et al., 2004). The two objectives for the DRM systems are to prevent unauthorized access to the digital content as it may cause an opportunity to produce an illegal copy and to provide mechanisms by which illegal copies can be detected and traced.

In order to fulfil the objective of the DRM system four requirements are to be met. First, the content is packed in a secure manner. Second, the access conditions for the protected content are specified. Third, a check has to be done on the access conditions. Finally, the protected content must be tamper-proof to circumvent or modify the security of the DRM system (E. I. Lin et al., 2005).

The DRM methods that are used to limit the use of digital content include encryption and watermarking techniques. Encryption provides authorized access to the digital content, which needs to be kept confidential. It converts the plaintext into ciphertext by scrambling the original data into unintelligible form with the help of a secret encryption key. Then this scrambled data or ciphertext is transmitted to the users from the content owners. The users on receiving the ciphertext have to perform the reverse process called as decryption to restore the original data or the plaintext with the help of a secret decryption key.

One of the drawbacks in the encryption process is that the ciphertext is very fragile. If the ciphertext is modified, or if parts of the ciphertext are lost during delivery, then the decryption process becomes impossible. Moreover the computational cost of video processing is increased if the content has to undergo the encryption and decryption process for secure delivery.

Watermarking is used for content protection and content tracking process. A watermark is an identity that is embedded with the help of a secret embedding key into the digital content and it describes the information about the content recipient. This implies that each user obtains a unique copy of the content. The embedded watermark must be robust and it is detected using a watermark detector with the help of a secret detection key. If a copy of the content is found in a suspicious location the embedded watermark can identify the source of the suspect copies. The watermarked content may be subjected to various attacks. An attack is a process of either removing the embedded watermark from the content or it may increase the difficulty in detecting the watermark and if such attacks are successful, then the benefits and protection that watermarking confers in the DRM system are lost. Another issue in watermarking is its computational cost. If different watermark have to be inserted into each copies of the digital content then the computational cost of embedding is a much greater concern.

The security of cryptography and watermarking techniques is reliant on ensuring secrecy of the keys and not by the secrecy of the encryption, decryption, watermark embedding, or watermark detection techniques. Thus, safeguarding the keys is very important to maintain the security of the DRM system. Unfortunately, implementing secure key management and exchange protocols to satisfy the above needs may add significant complexity to the DRM system.

The traitor tracing system is one of the key technologies that construct the DRM systems. It is the technique which is used to track the content usage and to confirm that no illegal distribution of the content exists. A traitor tracing scheme by using the efficient and computationally inexpensive public key cryptosystem NTRU is proposed in (LV

Xixiang et al., 2005). This scheme has the advantages of extremely efficient encryption and decryption, fast and easy key creation, low memory requirements and revocation property. Besides its high efficiency, this scheme also contains some other desirable features, such as collusion-resistant and black-box traceability.

A joint digital watermarking scheme using Chinese remainder theorem for the multiparty multilevel DRM architecture is proposed in (Tony Thomas et al., 2009). Multiparty multilevel digital rights management architecture involves several levels of distributors in between an owner and a consumer for digital content delivery. In the proposed scheme, watermark information is jointly created by all the parties involved; then a watermark signal is generated out of it and embedded into the content. This scheme takes care of the security concerns of all parties involved.

A secure multimedia distribution scheme for the converged Mobile TV services is proposed in (Shiguo Lian et al., 2010). This scheme will adopt both multimedia encryption and digital fingerprinting techniques to trace illegal redistributions. At the server side, the Joint Compression and Encryption method is proposed to encrypt video contents to get high efficiency. At the mobile terminal side, the Joint Decryption and Fingerprinting method is proposed to decrypt video contents and simultaneously embed the mobile terminal’s identification information to get high security. When the media content is illegally redistributed to public networks, such as Internet or public TV, the Fingerprint Detection and Traitor Tracing method will be used to identify the illegal redistributors.

Thus the various traitor tracing systems uses encryption and watermarking techniques, but since these techniques have their own drawback an additional technique is proposed in (Hidehisa Nakayama et al., 2010) to narrow down the list of users who may be traitors. In this system a method to track the content stream using information about traffic amount observed at routers is carried on. It also circumvents the need of decrypting and decoding the content and this is the major contrast with respect to the encryption and watermarking techniques.

III. PRIOR GUARANTEED RATE SCHEDULING ALGORITHMS

In this section different scheduling algorithms and their complexities are discussed. There are three switch architectures that an Internet router can use and they are the Input-Queued (IQ) switch, the Output-Queued (OQ) switch, or the Internally Buffered Crosspoint (IBC) switch and to minimize costs, most of the routers exploit IQ switch architecture. Scheduling for IQ switches is a difficult problem and it is presented in (V. Anantharam et al., 1999). Existing schedulers can be classified into two classes such as Dynamic schedulers and Guaranteed-Rate schedulers. A detailed analysis of the schedulers is presented in (Ted H. Szymanski et al., 2009) yet a brief discussion is as follows.

Dynamic schedulers for IQ switches can achieve optimal throughput, if a Maximum Weight Matching (MWM) algorithm is used to compute the matching for each time-slot. However, the algorithm has $O(N^3)$ complexity time and is considered computationally expensive for use in IP routers. Therefore, existing dynamic schedulers typically use sub-optimal heuristic schedulers. However, due to the severe time constraints all heuristic schedulers have sub-optimal throughput efficiencies and significant delay and jitter at high loads.

Guaranteed-Rate (GR) schedulers provide an alternative to dynamic schedulers and a generalized Guaranteed rate scheduling algorithm framework is discussed in (P. Goyal et al., 1997). A greedy scheduling algorithm with the goal to minimize the delay jitter on IP routers is introduced in (I. Keslassy et al., 2005; M. S. Kodialam et al., 2003), where a greedy low-jitter decomposition is performed with $O(N^3)$ time complexity. The resulting schedule of the algorithm requires a worst-case speedup of O(logN) and such hard analytic bounds on the jitter are not available. In the Birkoff von-Neuman (BVN) scheme which is proposed in (W. J. Chen et al., 2000), a doubly stochastic traffic rate matrix is decomposed into a sequence of permutation matrices and associated weights. These matrices are then scheduled using the GPS or WFQ algorithm to determine the sequence of switch configurations which meet the GR traffic requirements. But the BVN decomposition has a time complexity of $O(N^{4.5})$ and hence it is generally considered too slow for use in real-time IP routers.

In GR scheme that is proposed in (Ted H. Szymanski et al., 2009), a RSVP is used to maintain a traffic rate matrix for each IP router. The matrix is doubly stochastic, and specifies the guaranteed traffic rates between the IO ports of each packet-switched IP router. The matrix can then be processed to yield a sequence of switch permutations which can deliver the GR packets through the IP router according to delay and jitter constraints. Due to the recursive and fair nature of the scheduling algorithm the frame transmission schedules have very low delay jitter and hence this scheme is utilized in the IP routers to minimize the delay jitter while transmitting the streaming content to the users.

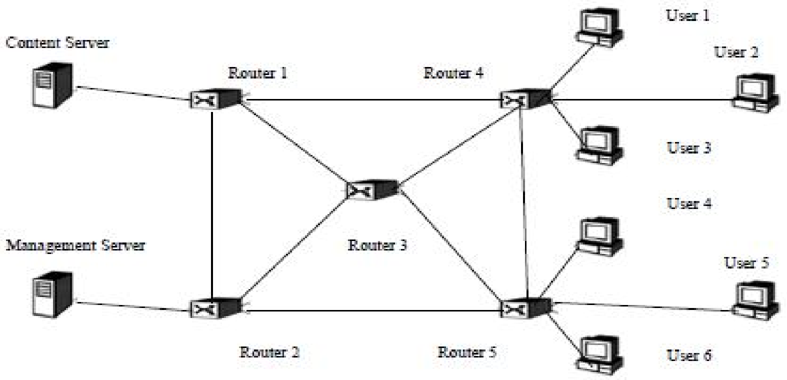
IV. MONITORING PROCESS OF THE TRAITOR TRACING SYSTEM

The proposed monitoring scheme is discussed in this section. The outline of the traitor tracing system is shown in Fig 1. The streaming content is transmitted from the Content Server to the different users through various routers. The traffic amount information is captured form the router near the content server and from the router near the respective users who are watching the content. The collected information include source IP address, source port number, destination IP address and destination port number and they are sent to the Management Server for further processing. On receiving the traffic amount information the Management Server constructs the traffic patterns for both the server and user side and then compares them to decide whether the user is watching the content or not.

If there exists a traitor in the network who illegally does a secondary distribution of the streaming content, this traffic would also pass through the same routers that are near the user and hence it would be captured and transmitted to the Management Server. The Management server then constructs the traffic pattern and compares it with the server side traffic pattern and detects the traitor. Thus this technique helps the content owner to securely transmit the streaming content to the intended users and achieve the objectives of the Digital Rights Management.

The construction of traffic patterns and the calculation of similarity between them are done as follows: At the server side the traffic amount information is continuously collected for the entire streaming process and at the user side it is collected for a specified time slot; hence the length of the user side observation time to capture the traffic amount is shorter than the server side. These collected information's are then expressed in terms of N dimension vector where N represents the length of the observation time.

Figure 1 Outline of the traitor tracing system.



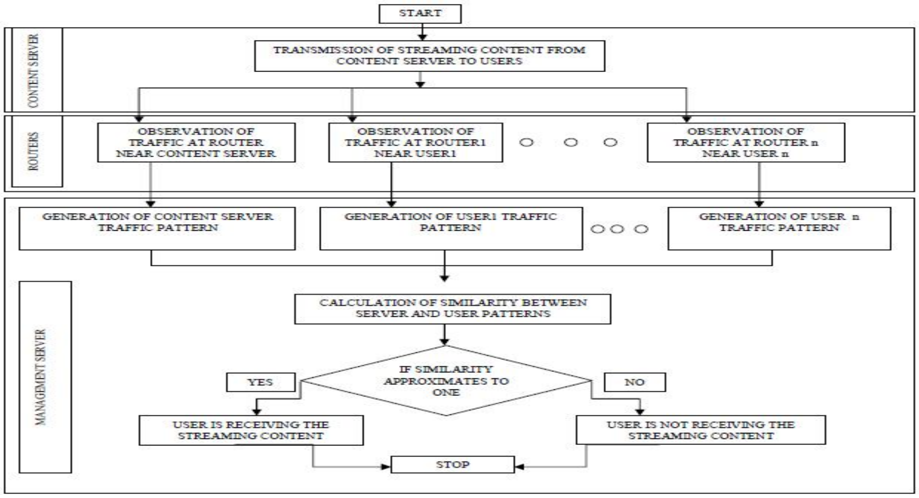
The server side traffic pattern is expressed as A_S where S is the length of the observation time for the server and user side traffic pattern is expressed as B_U where U is the length of the observation time for the user. The next step is to calculate the similarity between the patterns. From the server side a partial pattern A_U is extracted from A_S. The patterns A_U and B_U are then normalized as A'_u and B'_u and finally the similarity is calculated using the following equation which is referred from (Hidehisa Nakayama et al., 2010).

$R_{AB} = A'_u \, B'_u / \text{sqrt}\,(A'_u)^2 \, (B'_u)^2$.

If the value of R_{AB} approximates to 1 then there exists similarity between the server and user side traffic patterns. The Fig. 2 represents the above explained monitoring process in the form of a flowchart.

The computational cost of this monitoring process is relatively much less than the cost of encryption and watermarking techniques and hence it is more feasible to trace the traitors. But no network architecture is free from technical challenges such as delay, jitter and packet loss. When such a challenge is encountered in the monitoring process then the determination accuracy of the scheme might be affected. Even 2% delay jitter rate on the network starts to render the video stream unusable; therefore this would affect the calculation of similarity between the server and user side traffic patterns. Hence it becomes necessary to minimize the delay jitter to improve the determination accuracy of the monitoring process.

Figure 2 Flowchart representing the monitoring process.


START
CONTENT SERVER
TRANSMISSION OF STREAMING CONTENT FROM CONTENT SERVER TO USERS
ROUTERS
OBSERVATION OF TRAFFIC AT ROUTER NEAR CONTENT SERVER
OBSERVATION OF TRAFFIC AT ROUTER1 NEAR USER1
○ ○ ○
OBSERVATION OF TRAFFIC AT ROUTER n NEAR USER n
GENERATION OF CONTENT SERVER TRAFFIC PATTERN
GENERATION OF USER1 TRAFFIC PATTERN
○○○
GENERATION OF USER n TRAFFIC PATTERN
MANAGEMENT SERVER
CALCULATION OF SIMILARITY BETWEEN SERVER AND USER PATTERNS
IF SIMILARITY APPROXIMATES TO ONE
YES
NO
USER IS RECEIVING THE STREAMING CONTENT
USER IS NOT RECEIVING THE STREAMING CONTENT
STOP

V. SCHEDULING ALGORITHM

The Guaranteed Rate scheduling algorithm to minimize the delay jitter is referred from (Ted H. Szymanski et al., 2009) and discussed in this section. In an IP router which uses an IQ crossbar switch the packets containing the streaming content arrive at the input ports. Each packet is disassembled into cells and stored in the appropriate Virtual output queues (VOQ) at the input side of the router. Each VOQ (x,y) stores cells at input port x destined for output port y. The packets are transmitted across the IQ switch in a series of time-slots. The packets are reconstructed at the output side of the router and transmitted to the next router in the network. In each time-slot, the scheduling algorithm is used to compute the number of packets to transmit across an IQ switch.

A IxJ packet switch in the router consists of I input and J output ports and an associated traffic rate matrix which is doubly stochastic. A doubly stochastic matrix is a square matrix of nonnegative real numbers and each element in the matrix represents the fraction of the transmission line rate reserved for GR traffic between IO pair (I,J). The scheduling algorithm converts this doubly stochastic traffic rate matrix into a quantized matrix where each traffic rate is expressed as an integer number times the minimum quota of reservable bandwidth, for a scheduling frame of length F timeslots.

The algorithm then recursively partitions the quantized matrix in a relatively fair manner, to yield a sequence of permutations which represents the switch configurations. The resulting sequence is called as 'frame transmission schedule' and it is used for transmitting packets through the router. The computed frame transmission schedule is repeatedly re-used, as long as the traffic rate matrix remains unchanged and the same is recomputed when the traffic rate matrix is updated by the RSVP.

The recursive and fair nature of the scheduling algorithm computes the frame transmission schedules that have very low delay jitter. The delivery of a packetized multimedia stream with very low delay jitter would be possible if the following 2 conditions can be met: (a) each frame transmission schedule is relatively fair such that no packets wait excessively long for transmission and (b) each router buffers a sufficient number of packets to compensate for any transmission lead/lag. Under these conditions, the multimedia stream flow will be transmitted through each IP router in a deterministic pattern, where the delay and jitter are minimized.

The Guaranteed Rate scheduling algorithm is discussed below.

GUARANTEED RATE SCHEDULING ALGORITHM

Step 1: Given a traffic rate matrix R, create doubly-stochastic matrix R(tilde) and create quantized rate matrix M for a frame length F.

Step 2: Recursively decompose matrix M, to yield a sequence of permutations and the same is used to configure the IQ switch.

Step 3: Repeat the sequence of permutations until the traffic rate matrix remains unchanged.

Step 4: If the traffic rate matrix is updated by the RSVP then the sequence of permutations are recomputed.

The algorithm to convert any doubly sub stochastic traffic rate matrix into a doubly stochastic traffic rate matrix is discussed below.

MATRIX CONVERSION ALGORITHM

Step 1: If the sum of all elements in R < N, then there exists an element r(i,j) such that row_sum < 1.0 and col_sum < 1.0

Find the element r(i,j) and compute epsilon = 1 – max[row_sum, col_sum]

Step 2: Add epsilon to r(i,j), which causes either the row_sum = 1.0 or col_sum = 1.0
Step 3: Repeat the above steps until the sum of all elements = N.

The algorithm to decompose any doubly stochastic traffic rate matrix into a sum of weighted permutation matrices is discussed below.

MATRIX DECOMPOSITION ALGORITHM

Step 1: Given a doubly stochastic matrix R, let (i1, i2,….,iN) be a permutation of (1, 2,….,N). Step 2: Let P1 be the permutation matrix corresponding to (i1,i2,….,iN) and define Φ_1 = min1≤k≤N ($\tilde{r}$ k,ik) and R1 = R - Φ_1 . P1 Step 3: If R1 = 0 then the decomposition is complete

Step 4: Otherwise, If $\Phi_1 < 0$ then R2 = 1/ (1- Φ_1) R1 is still doubly stochastic and the decomposition can proceed from step 1 Iterate Step 1 to 4 until termination.

The algorithm to schedule the permutation matrices is discussed below.

SCHEDULING OF PERMUTATION MATRICES

Step 1: Set discrete time-slot n = 1 initially. Given each permutation k a finishing time F(k,1) = 1/Φ_k
Sort the k tokens in order of increasing finishing times.

Step 2: Select the smallest token, F(k,c), schedule permutation k for time-slot n and increment time n.

Step 3: Assign the token a new Finishing Time F(k,c+1) = F(k,c) + 1/ Φ_k and insert the token into the sorted list.

Thus the Guaranteed Rate scheduler scheme is utilized to minimize the delay jitter in the network and to improve the determination accuracy of the monitoring process.

V. PERFORMANCE ANALYSIS WITH SIMULATIONS

In this section, we will study the performance of the traitor tracing system through various simulations. The simulations are done in NS2 (Chih-Heng Ke et al 2008). The various performance measures that are used in the traitor tracing system are CR, TR, MS, where CR is the number of users who are authorized to watch the streaming content and are watching, TR is the number of users who are illegally watching the streaming content and MS is the number of authorized users to watch the content but not able to watch due to delay jitter or packet loss. The above mentioned measures are used to compute the performance metrics such as recall, precision, miss out and f score.

$$\text{Recall } R = (CR/CR+MS) \text{ X } 100\ [\%]$$

$$\text{Precision } P = (CR/CR+TR) \text{ X } 100\ [\%]$$

$$\text{Miss ratio} = (MS/CR+MS) \text{ X } 100\ [\%]$$

$$\text{F score} = (2 * R * P) / (R+P)$$

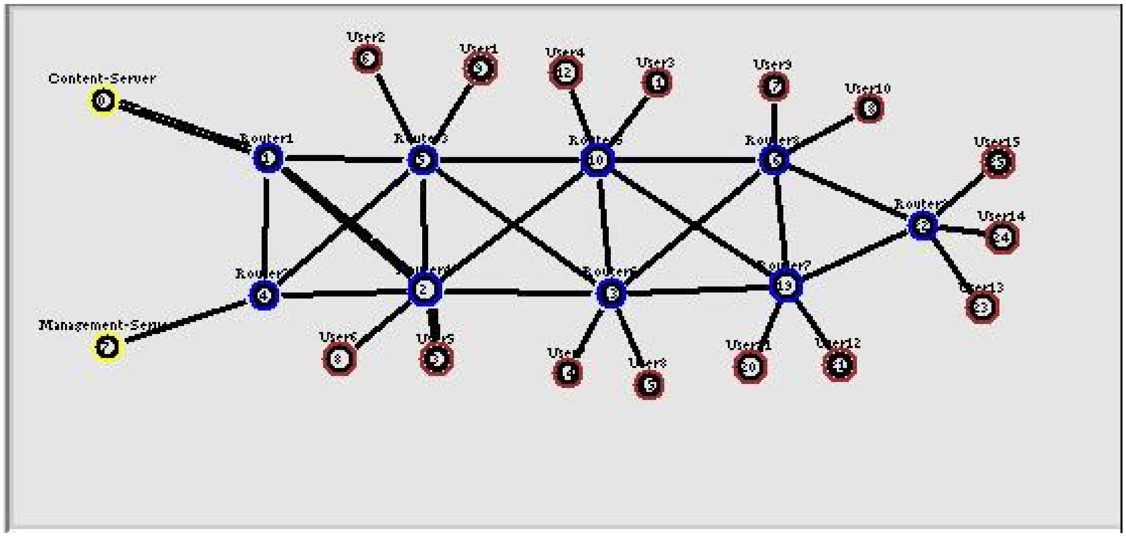
Large values of recall, precision and f score metrics and small values of miss out metric prove high performance of the traitor tracing system. The Table I shows the hardware and software requirements used to simulate the process.

TABLE I

H/W AND S/W REQUIREMENTS

H/W or S/W	Specification
CPU	Intel Core i3
RAM	4GB
OS	RedHat Linux 9
NS2	2.29

Figure 3 Simulation setup.



The simulation setup is shown in Fig. 3 and it consists of 2 servers, 9 routers and 15 users. Node 0 is the Content Server which sends the streaming video content to the users. Node 7 is the Management Server which finds the traffic pattern similarity matching between server and user. Nodes 1, 2, 4, 5, 10, 13, 16, 19 and 22 are the routers and Nodes 3, 6, 8, 9, 11, 12, 14, 15, 17, 18, 20, 21, 23, 24 and 25 are the users who might watch the streaming video content.

In the simulation the streaming content is delivered from the Content server to the various users. The Router1 captures the traffic amount information on the server side and routers near the users capture the same on the user side. These information are then sent to the Management Server where the construction of traffic patterns and the calculation of similarity between them are performed. The performance evaluation of the monitoring process is then done based on the various performance measures and metrics.

During the streaming process congestion rises in the network due to improper scheduling of streams and hence it leads to packet loss. The user when he watches such a stream the perceived quality of the video would be low and he would also miss certain parts of the video. This situation can still get worse in the existence of traitors has they would try to grab the packets from the routers near the users causing more traffic in the network. On the other hand the traffic pattern matching done on the Management server will also become a problem, because the traffic amount information captured from the router near the user might not be effective since packet loss has happened. Due to this problem the determination accuracy of the monitoring process decreases. To overcome these problems the Guaranteed Rate scheduling algorithm is implemented. This algorithm manages the scheduling of switches based on the information computed from the traffic rate matrix of the different routers. Once this is done the performance evaluation of the monitoring process was once again done to check whether the determination of traitors was increased.

Using the above mentioned setup 10 different simulation was run with different performance measures. The values of the performance measures and its evaluated metrics are represented in the Table II and III. Table II values are considered before implementing the scheduling algorithm and Table III values are considered after implementing the scheduling algorithm. Based on this performance metric evaluation the recall, precision, f score and miss out graphs are drawn. After the simulation is run the trace file is generated and using the information from this the delay, jitter and throughput graphs are drawn.

The performance metrics such as recall, precision, f score and miss out are represented as graphs in Fig. 4, 5, 6 and 7. The minimization of delay and jitter are represented as graphs in Fig 8 and 9 and throughput is represented as graph in Fig 10.

The analysis of the results of the different simulation scenarios after implementing the Guaranteed Rate scheduling algorithm leads to the following:

- 10% increase in recall performance metric.
- 2% increase in precision performance metric.
- 6% increase in f score performance metric.
- 10% decrease in miss out performance metric.
- 1.3% decrease in delay performance metric.
- 1.03% decrease in jitter performance metric.

Hence it concludes that the performance of the determination accuracy of the monitoring process of traitor tracing system is increased after the minimization of the delay jitter using the Guaranteed Rate scheduling algorithm.

TABLE II

PERFORMANCE MEASURES AND METRICS BEFORE IMPLEMENTING THE GUARANTEED RATE SCHEDULING ALGORITHM.

CR	TR	MS	RECALL BEFORE	PRECISION BEFORE	F SCORE BEFORE	MISS OUT BEFORE
15	0	0	100	100	100	0
14	1	1	93	93	93	7
14	1	1	93	93	93	7
13	1	2	87	93	90	13
13	2	2	87	87	87	13
12	2	3	80	86	83	20
12	2	3	80	86	83	20
11	1	4	73	92	81	27
11	1	4	73	92	81	27
10	1	5	67	91	77	33

TABLE III

PERFORMANCE MEASURES AND METRICS AFTER IMPLEMENTING THE GUARANTEED RATE SCHEDULING ALGORITHM.

CR	TR	MS	RECALL AFTER	PRECISION AFTER	F SCORE AFTER	MISS OUT AFTER
15	0	0	100	100	100	0
15	0	0	100	100	100	0
15	1	0	100	94	97	0
14	1	1	93	93	93	7
14	2	1	93	88	90	7
14	2	1	93	88	90	7
14	1	1	93	93	93	7
13	1	2	87	93	90	13
13	1	2	87	93	90	13
13	1	2	87	93	90	13

Figure 4 Recall graph.

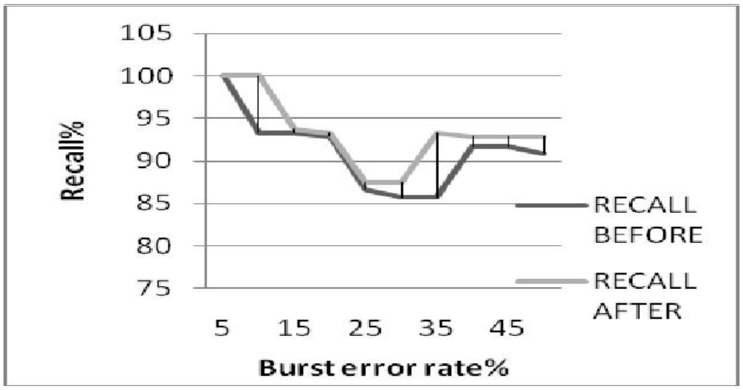


Figure 5 Precision graph.

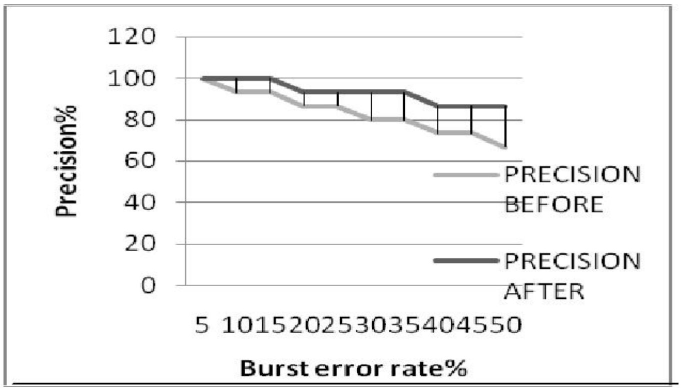


Figure 6 Miss out graph.

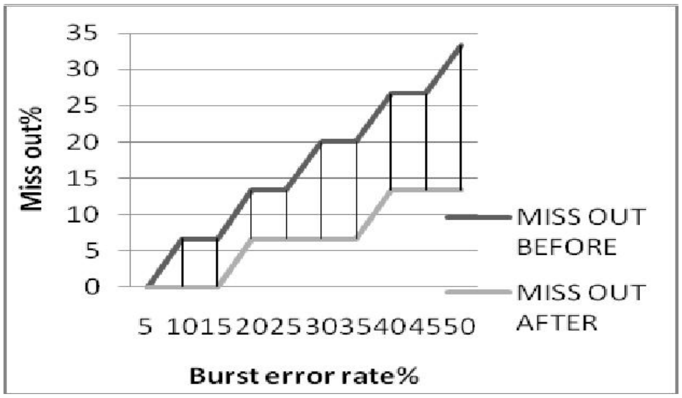


Figure 7 F score graph.

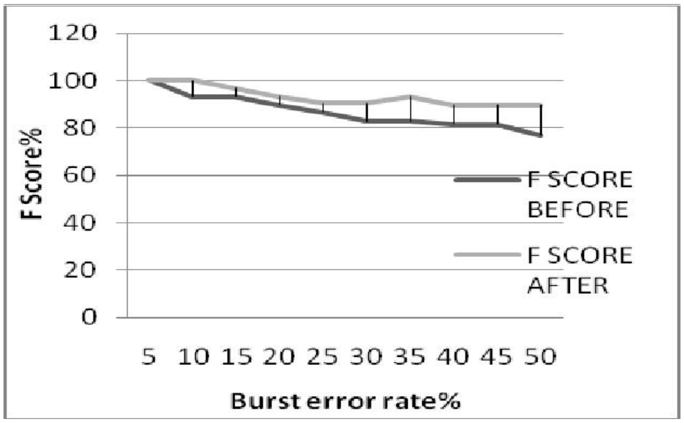


Figure 8 Delay graph.

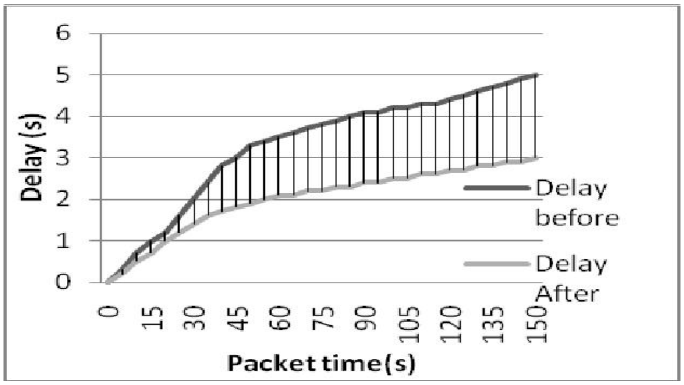


Figure 9 Jitter graph.

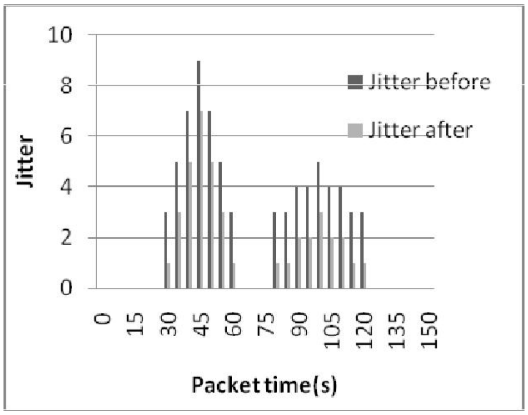
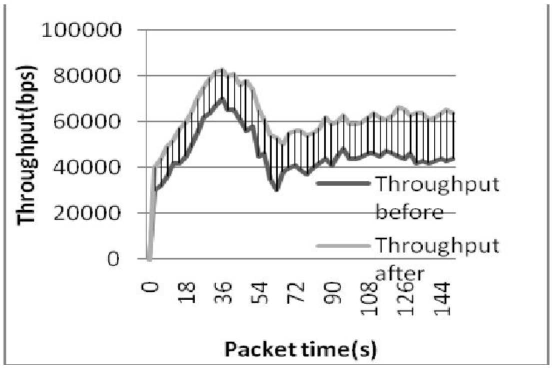


Figure 10 Throughput graph.



VI. Conclusion and Future Work

In today's world the protection of digital content becomes a challenging task for the DRM systems. The discussion about existing traitor tracing techniques implies that, there exist drawbacks either in terms of cost or in maintaining the security of keys involved in encryption and watermarking techniques. Hence in this paper a new Traitor tracing technology is presented to securely transmit the streaming contents to the users with essentially low delay jitter. The technology uses a monitoring process which monitors the amount of traffic on the routers near the servers and users. The collected information are then used to construct the traffic patterns. Finally the calculation of similarity between the server and user side traffic patterns are computed to detect whether the user is watching the streaming content or not and thereby protects the digital content from secondary or illegal distributions. In the proposed process the minimization of delay jitter is also achieved through Guaranteed Rate scheduler scheme. The simulation results depicts the performance evaluation o f the process and it also concludes that the performance of the traitor tracing system increases after the minimization of the delay jitter.

The proposed scheme protects the streaming content without intercepting the data inside the packets and hence the privacy of the content is maintained, therefore this method can be used to secure resources that are being shared across the world. Thus the future direction could be to extend the monitoring process to resolve the security and privacy issues in the cloud environment.

REFERENCES.

[1] H. Cheng and X. Li. (2000) 'Partial encryption of compressed images and videos', IEEE Trans. Signal Process., vol. 48, no. 8, pp. 2439–2451.
[2] A. Pommer and A. Uhl. (2003) 'Selective encryption of wavelet-packet encoded image data: Efficiency and security', Multimedia Syst., vol. 9, no. 3, pp. 279–287.
[3] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu. (2003) 'Anti-collusion fingerprinting for multimedia', IEEE Trans. Signal Process., vol. 51, no. 4, pp. 1069–1087.
[4] D. Boneh and J. Shaw. (1998) 'Collusion-secure fingerprinting for digitaldata', IEEE Trans. Inf. Theory, vol. 44, no. 5, pp. 1897–1905.
[5] R. S. Naini and Y.Wang. (2003) 'Sequential traitor tracing', IEEE Trans. Inf. Theory, vol. 49, no. 5, pp. 1319–1326.
[6] K. Su, D. Kundur, and D. Hatzinakos. (2005) 'Statistical invisibility for collusion-resistant digital video watermarking', IEEE Trans. Multimedia, vol. 7, no. 1, pp. 43–51.
[7] M. Barni and F. Bartolini. (2004) 'Data hiding for fighting piracy', IEEE Signal Process. Mag., vol. 21, no. 2, pp. 28–39.
[8] B. N. Park, W. Lee, and J. W. kim. (2005) 'A license management protocol for protecting user privacy and digital contents in digital rights management systems', IEICE Trans. Inf. Syst., vol. E88-D, no. 8, pp. 1958–1965.
[9] M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour. (2006) 'Traitor tracing technology of streaming contents delivery using traffic pattern in wired/wireless environments', in Proc. IEEE GLOBECOM, pp. 1–5.
[10] Hidehisa Nakayama, Abbas Jamalipour and Nei Kato. (2010) 'Network-Based Traitor-Tracing Technique Using Traffic Pattern', IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 2.
[11] S. Chand and H. Om. (2007) 'Modeling of buffer storage in video transmission', IEEE Trans. Broadcasting, vol. 53, no. 4, pp. 774–779.
[12] Ted H. Szymanski and Dave Gilbert. (2009) 'Internet Multicasting of IPTV With Essentially-Zero Delay Jitter', IEEE TRANSACTIONS ON BROADCASTING, VOL. 55, NO. 1.
[13] F. Hartung and F. Ramme. (2000) 'Digital rights management and watermarking of multimedia content for m-commerce applications', IEEECommun. Mag., vol. 38, no. 11, pp. 78–84.
[14] R. H. Koenen, J. Lacy, M. Mackay, and S. Mitchell. (2004) 'The long march to interoperable digital rights management', Proc. IEEE, vol. 92, pp. 883–897.
[15] E. I. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp. (2005) 'Advances in digital video content protection', Proc. IEEE, vol. 93, no. 1, pp. 171–183.
[16] LV Xixiang, YANG Bo and Changxing Pei. (2005) 'Efficient Traitor Tracing Scheme Based On NTRU', Proceedings of the Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'05).
[17] Tony Thomas, Sabu Emmanuel, A. V. Subramanyam, and Mohan S. Kankanhalli. (2009) 'Joint Watermarking Scheme for Multiparty Multilevel DRM Architecture', IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.
[18] Shiguo Lian and Xi Chen. (2010) 'Secure and traceable multimedia distribution for convergent Mobile TV services', Elsevier.
[19] V. Anantharam, N. McKeown, A. Mekittikul, and J. Walran. (1999) 'Achieving 100% throughput in an input queued switch', Trans.Comm., vol. 47, no. 8, pp. 1260–1267.
[20] P. Goyal and H. M. Vin. (1997) 'Generalized guaranteed rate scheduling algorithms: A framework', IEE/ACM Trans. Networking, vol. 5, no. 4, pp. 561–571.
[21] I. Keslassy, M. Kodialam, T. V. Lakshamn, and D. Stiliadis. (2005) 'On guaranteed smooth scheduling for input-queued switches', IEEE/ACM Trans. Networking, vol. 13, no. 6, pp. 1364–1375.
[22] M. S. Kodialam, T. V. Lakshman, and D. Stilladis. (2003) 'Scheduling of Guaranteed-Bandwidth Low-Jitter Traffic in Input-Buffered Switches', US Patent Application #20030227901.
[23] W. J. Chen, C.-S. Chang, and H.-Y. Huang. (2000) 'Birkhoff-von Neumann input buffered crossbar switches', in Proc. Infocom.
[24] VINTproject, Network simulator 2. Available at: http://www.isi.edu/nsnam/ns/.
[25] Chih-Heng Ke, Ce-Kuen Shieh, Wen-Shyang Hwang and Artur Ziviani. (2008) 'An Evaluation Framework for More Realistic Simulations of MPEG Video Transmission', JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 24, 425-440.