# Achieving of Effective Video Streaming by User Privacy Management

**P.MADHUSUDHANA RAO**
M.Tech Student, Dept of CSE
Vidya Vikas Institute of Technology
Chevella, T.S, India

**M.ANUSHA**
Assistant Professor, Dept of CSE
Vidya Vikas Institute of Technology
Chevella, T.S, India

**D.KOTESWARA RAO**
Associate Professor & HOD, Dept of CSE
Vidya Vikas Institute of Technology
Chevella, T.S, India

**Dr. J.SASI KIRAN**
Professor & Dean, Dept of CSE,
Vidya Vikas Institute of Technology
Chevella, T.S, India

*Abstract:* **Due to popularity of streaming applications in recent years, reliable video delivery to suspend objectionable content-leakage has, certainly, turn out to be important. Traffic patterns with reference to streaming videos symbolize the skeleton carrying their features and are exceptional per content. In our work we focus on illicit redistribution of streaming content by means of an allowed user towards external networks. By comparing videos of distinctive length, in our work we determine a relationship among length of videos to be evaluated and their resemblance. In our work we suggest an innovative content-leakage detection system that is robust to variation of video length. The system that was introduced assist in flexible as well as precise streaming content leakage detection regardless of length of streaming content, which improve secured and trustworthy content delivery.**

*Keywords:* **Streaming applications, Content leakage, Video delivery, Traffic patterns.**

## I. INTRODUCTION

In recent times, due to rapid development of broadband technologies and development of high-speed networks, recognition of instantaneous applications of video streaming applications has gained attention [1]. An important concern in video streaming services is fortification of bit stream from illegal use, as well as distribution. One of the most well-liked approaches to put off objectionable contents distribution towards unofficial users to look after authors' copyrights is digital rights management technology. For the most part of digital rights management techniques make use of cryptographic or else digital watermark techniques. On the other hand these methods have no important effect on rearrangement of contents, restored at user-side by approved yet malicious users. Redistribution is precisely no longer difficult by means of peer-to-peer streaming software for this reason; streaming traffic might be escaped to peer-to-peer networks. Instantaneous video streaming communications by means of virtual private networks are being extensively deployed in huge number of corporations as a commanding means of resourcefully promoting business activities devoid of additional costs [2][3]. The continuation of videos with reference to different length within network environment causes a substantial degradation in performance of leakage detection. In our work we spotlight on illegitimate redistribution of streaming content by means of an allowed user towards external networks. The existing proposals in literature scrutinize information that is obtained at different nodes in core of streaming path. As a result, expanding an innovative leakage detection technique strong to difference of video lengths is, really necessary. In our work by comparing videos of different length, we determine a relationship among length of videos to be evaluated and their resemblance and based on this relationship, decision threshold enabling precise leakage detection was determined even in an environment by different length videos.

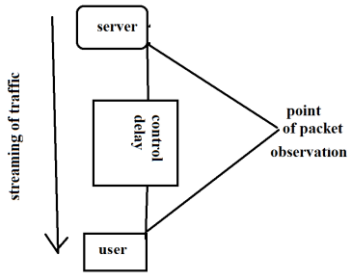


***Fig1: An overview of streaming of traffic.***

## II. METHODOLOGY

The content leakage detection system on the basis of fact that streaming content encompasses an exceptional traffic pattern is a pioneering solution to put off illegal redistribution of contents by means of a regular, yet malicious user. While protecting user privacy, traditional systems have proposed methods on the basis of observation concerning streamed traffic all the way through network. These conventional systems preserve high detection accurateness while coping with some of traffic distinction in network, on the other hand, their detection performance considerably degrade

  

owing to important variation of video lengths. In our work we put forward a new content-leakage detection system that is robust to variation of video length. By comparison of videos of different lengths, we determine a relationship among length of videos to be evaluated and their resemblance among the compared videos. Thus, we improve detection performance of projected scheme even in an environment subjected to dissimilarity in length of video. The existence of videos concerning different length within network environment causes a substantial degradation in performance of leakage detection. Traditional methods are time slot-based traitor tracing, packet size-based traitor tracing, as well as dynamic programming-based traitor tracing. The proposed scheme allows flexible as well as precise streaming content leakage detection regardless of length of streaming content, which improve secured and trustworthy content delivery [4]. In typical video leakage state of affairs because of popularity of streaming delivery of movies, expansion of peer to peer streaming software has concerned much attention. In the typical content-leakage scenario a regular user in a protected network accept streaming content from a content server. Subsequently, by means of use of peer to peer streaming software, usual yet malevolent user redistributes streaming content towards a non-regular user outer surface its network and such content-leakage is almost not detected.

## III. MODELLING OF PROPOSED SYSTEM

Although protecting user privacy, traditional systems have proposed methods on the basis of observation concerning streamed traffic all the way through network. Traffic patterns concerning streaming videos symbolize the skeleton carrying their features and are exceptional per content. As a result, the longer the traffic pattern is; the additional information on video it exhibits. In traditional methods, it is supposed that a convinced length of content can constantly be obtained all the way through the network for the entire contents. We set up a new threshold determination method on basis of exponential approximation. The projected decision threshold determination method is put into practice into dynamic programming-based traitor tracing which employs packet size-based traffic generation algorithm since dynamic programming-based traitor tracing illustrates high robustness to network environment changes when compared to other schemes. In network topology of projected leakage detection system topology consists of two most important components, specifically the traffic pattern generation engine fixed in each router, and traffic pattern matching engine put into practice in the management server. Traffic pattern generation procedure is based on moreover time slot-basis algorithm or packet size-based algorithm. Time slot-based algorithm is a simple solution to produce traffic patterns by summing quantity of traffic arrival throughout a certain period of time. Consequently, delay as well as jitter of packets disfigure traffic pattern, and hence, decreases precision in pattern matching [5]. Time slot-based algorithm is influenced by packet loss. Algorithm of packet size-basis defines a slot as summing up of quantity of arrival traffic until observation of a convinced packet size and this algorithm only utilize packet arrival order as well as packet size, thus is strong to modify in environment for instance delay and jitter. Packet size-based algorithm demonstrates no toughness to packet loss. Traditional methods are time slot-based traitor tracing, packet size-based traitor tracing, as well as dynamic programming-based traitor tracing. Time slot-based pattern generation algorithm that is employed within time slot-based traitor tracing is influenced by packet delay as well as jitter, which get worse user-side traffic pattern. Packet size-based traitor tracing, as well as dynamic programming-based traitor tracing make use of a traffic pattern generation means based on packet size rather than time slot therefore, show robustness in opposition to packet delay as well as jitter. although three representative conventional methods, that is, time slot-based traitor tracing, packet size-based traitor tracing, as well as dynamic programming-based traitor tracing demonstrate toughness to delay, jitter or else packet loss, detection performance reduce with substantial variation of video lengths [6].

## IV. CONCLUSION

A vital issue regarding video streaming services is fortification of bit stream from illegal use, as well as distribution. Digital rights management technology is the one of most popular approaches to suspend objectionable contents distribution towards unofficial users to look after authors' copyrights. In established methods, it is supposed that a convinced length of content can constantly be obtained all the way through the network for the entire contents. Immediate communications of video streaming by means of virtual private networks are being expansively deployed in huge number of corporations as a commanding means of resourcefully promoting business activities devoid of additional expenses. We draw attention towards illegitimate redistribution of streaming content by means of an allowed user towards external system. In our work by comparing videos of different length, we determine a relationship among length of videos to be evaluated and their resemblance. In our work we suggest a new content-leakage detection system that is robust to variation of video length. We get better detection performance of projected scheme even in an environment subjected to dissimilarity in length of video. The proposed system allows flexible as well as precise streaming

  

content leakage detection regardless of length of streaming content, which improve secured and trustworthy content delivery.

## V. REFERENCES

[1] O. Adeyinka, "Analysis of IPSec VPNs Performance in a Multimedia Environment," Proc. Fourth Int'l Conf. Intelligent Environments, pp. 25-30, 2008.

[2] E.I. Lin, A.M. Eskicioglu, R.L. Lagendijk, and E.J. Delp, "Advances in Digital Video Content Protection," Proc. IEEE, vol. 93, no. 1, pp. 171-183, Jan. 2005.

[3] S. Craver, N. Memon, B.L. Yeo, and M.M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications," IEEE J. Selected Areas Comm., vol. 16, no. 4, pp. 573-586, May 1998.

[4] Y. Liu, Y. Guo, and C. Liang, "A Survey on Peer-to-Peer Video Streaming Systems," Peer-to-Peer Networking and Applications, vol. 1, no. 1, pp. 18-28, Mar. 2008.

[5] E.D. Zwicky, S. Cooper, and D.B. Chapman, Building Internet Firewalls, second ed., O'Reilly and Assoc., 2000.

[6] 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.

## AUTHOR's PROFILE

**P.MADHUSUDHANA RAO,** completed my B.tech from SRI SHIVANI college of Engg . I am pursuing M.Tech in vidya vikas institute of technology. My Hobbies are Reading books.

**Mrs. M. Anusha** Graduated in B.Tech [CSE] from JNTU Hyd. She received Masters Degree in M. Tech from JNTU Hyd. Her Interested areas are Wireless Sensor Networks, Computer Organization, Network Security and ryptography. Currently, she is working as an Assistant Professor in Vidya Vikas Institute of Technology.

**D.Koteswara Rao** Graduated in B.Tech CSE from JNTU Hyd. He received Masters Degree in M.Tech [CSE] from Nagarjuna University, Guntur. Currently he is working as Associate Professor in CSE in Vidya Vikas Institute of Technology, Chevella, R.R. Dist Telangana State, India. His research interests include Formal Languages and Automata Theory. He has published research papers in various National, International Conferences, Proceedings and Journals. He has received best Teacher award from Vidya Group.

**Dr. J. Sasi Kiran** Graduated in B.Tech [EIE] from JNTU Hyd. He received Masters Degree in M.Tech [Computers & Communications] from Bharath University, Chennai, M.Tech [CSE] from JNT University, Hyderabad. He received Ph.D degree in Computer Science from University of Mysore, Mysore. He has served Vidya Vikas Institute of Technology for 10 years as Assistant Professor, Associate Professor, HOD-CSE&IT & Vice Principal and taught courses for B.Tech and M.Tech Students. At Present he is working as Professor in CSE and Dean – Academics in Vidya Vikas Institute of Technology, Chevella, Greater Hyderabad, R.R. Dist Telangana State, India. His research interests include Image Processing, Cloud Computing and Network Security. He has published several research papers till now in various National, International Conferences, Proceedings and Journals. He is a life member of CSI, ACM, ISTE, IE, IAE, NSC, ISCA, IACSIT, CSTA, AIRCC, CRSI, GMIS-USA, Red Cross and Managing Committee Member of Computer Society of India. He has an editorial board member of IJERT and board of studies member of CVSR Engineering College, Hyd. He has received best Teacher award twice from Vidya Group, Significant Contribution award from Computer Society of India and Passionate Researcher Trophy from Sri. Ramanujan Research Forum, GIET, Rajuhmundry, A.P, India.

  