Traffic Pattern-Based mostly Content Leak Detection for Trustworthy Content Delivery Networks

Sapkal Pratiksha Sharad
Department of Computer Engineering
Brahma Valley college of Engineering and Research Institute
Nashik, Maharashtra
Email: pratikshasapkal10@gmail.com

Jagdio Simran Jagjeet Singh
Department of Computer engineering
Brahma valley College of Engineering and Research Institute
Nashik, Maharashtra
Email: simranjagdev16@gmail.com

Ghaywat Vaishali Navnath
Department of Computer Engineering
Brahma Valley College of Engineering and Research Institute
Nashik, Maharashtra
Email:vaishalinghaywat1995@gmail.com

Rule Sujata Dinesh
Department of Computer Engineering
Brahma Valley College of Engineering and Research Institute
Nashik, Maharashtra
Email: sujatarule171994@gmail.com

Abstract**—**Due to the increasing quality of transmission streaming applications and services in recent years, the difficulty of sure video delivery to stop undesirable content-leakage has, indeed, become crucial. While conserving user privacy, typical systems have addressed this issue by proposing strategies supported the observation of streamed traffic throughout the network.These standard systems maintain a high detection accuracy whereas managing a number of the traffic variation within network delay and packet loss and their detection performance well degrades thanks to the many variation of video lengths.In this paper, we focus on the solution overcoming this issue by proposing a unique content-leakage detection theme that's strong to the variation of the video length.By comparison videos of various lengths, we tend to confirm a relation between the length of videos to be compared and also the similarity between the compared videos.Therefore, we tend to enhance the detection performance of the projected theme even in associate degree setting subjected to variation long of video.Through a experimentation and testing procedure , the potential of achieving of our projected theme is evaluated in terms of variation within the length of video , delay in qualities of video, and loss of packets.

Keywords-*Streaming content, leak Detection, itinerary, Degree of Similarity*

*****

I. Introduction

I N recent years, with the speedy development of broadband technologies and also the advancement of high-speed wired/ wireless networks, the recognition of time period video streaming applications and services over the net has inflated by leaps and bounds.YouTube and microsoft network video square measure notable samples of such applicationsThey Serve an oversized population of users from all around the world with diverse contents, ranging from daily news feeds to entertainmentfeeds to amusement feeds together with music, videos, sports,and so forth, by using streaming transmission technologies.In addition, period video streaming communications like internet conference in intracompany networks or via net with virtual non-public networks (VPNs) area unit being wide deployed in an exceedingly sizable amount of firms as a strength requiring means that of expeditiously raising and encouraging business activities while not further prices.A essential concern in video reception or playback of video services is that the protection of the bit stream from unauthorized use, duplication and distribution.One of the foremost well-liked approaches to stop undesirable contents distribution to unauthorized users and/or to guard author's copyrights is related to digital rights management (DRM) technology.Most DRM techniques use cryptological or digital watermark techniques. However, this sort of approaches don't have any vital result on distribution of contents, decrypted or remodeled at the user-side by approved nonetheless malicious users..Moreover, distribution is technically now not burdensome by victimization peer-to-peer (P2P) streaming code . Hence, streaming traffic could also be leaked to peer-to-peer networks. On the opposite hand, packet filtering by firewall-equipped egress nodes is a straightforward resolution to avoid outflow of streaming contents to external networks.In this resolution, the packet header data (e.g., destination and supply net protocol addresses, protocol sort, and port range of outgoingness of traffic) of each streamed packet is inspected. just in case the inspected packets don't verify the predefined filtering policy, they're blocked and bornHowever, it's tough to completely stop streaming content outflow by means that of packet filtering alone as a result of the packet header data of malicious users is such-and-such beforehand and may be simply spoofed. During this paper, we tend to concentrate on the extrajudicial distribution of streaming content by a licensed user to external networks.The existing proposals in and monitor data obtained at completely different nodes within the middle of the streaming path. The retrieved data area unit accustomed generate traffic patterns that seem as distinctive wave shape per content similar to a fingerprint.The generation of itinerary doesn't need any info on the packet header, and so preserves the user’s privacy. escape detection is then performed by examination the generated traffic patterns.. However, the existence of videos of various length within the network surroundings causes a substantial degradation within the escape detection performanceThus, developing AN innovative outflow detection methodology sturdy to the variation of video lengths is, so needed. during this paper, by examination completely different length videos, we have a tendency to verify a relationship between the duration of videos to be compared and their similarity or relation of sharing properties. supported this relationship, we have a tendency to verify call threshold sanctionative correct outflow detection even in AN atmosphere with completely different length videos.

II. Literature Survey

One of the foremost standard approaches to stop undesirable contents distribution to unauthorized users is the technology of Digital Rights Management. Most DRM techni-ques use scientific discipline or digital watermark techniques. However, this sort of approaches don't have any vital impact on distribution of contents, decrypted or improved at the user-side by approved however malicious users.

1) summary of the H.264/AVC video secret writing normal

AUTHORS: T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra

H.264/AVC is newest video secret writing normal of the ITU-T Video secret writing consultants cluster and therefore the ISO/IEC motion picture consultants cluster. the most goals of the H.264/AVC standardization effort are increased compression performance and provision of a "network-friendly" video illustration addressing "conversational" (video telephony) and "nonconversational" applications. H.264/AVC has achieved a big improvement in rate-distortion potency relative to existing standards. this text provides an summary of the technical options of H.264/AVC, describes for the quality, and descriptions the history of the standardization method.

2) A high output path metric for multi-hop wireless routing

AUTHORS: D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris

This paper presents the estimated transmission count metric (ETX), that finds high-throughput ways on multi-hop wireless networks. ETX minimizes the expected total range of packet transmissions (including retransmissions) needed to with success deliver a packet to the final word destination. The ETX metric incorporates the consequences of link loss ratios, spatial property within the loss ratios between the 2 directions of every link, and interference among the sequential links of a path. In distinction, the minimum hop-count metric chooses randomly among the various ways of a similar minimum length, notwithstanding the usually massive variations in output among those ways, and ignoring the likelihood that a extended path would possibly provide higher output.This paper describes the planning and implementation of ETX as and DSR routing protocols, moreover as modifications to DSDV and DSR which permit them to use ETX. Measurements taken from a 29-node 802.11b test-bed demonstrate the poor performance of minimum hop-count, illustrate the causes of that poor performance, and make sure that ETX improves performance. For long ways the output improvement is usually an element of 2 or a lot of, suggesting that ETX can become a lot of helpful as networks grow larger and ways become longer.

3) Packet loss resilient transmission of MPEG video over the web

AUTHORS: J. M. Boyce

A method is projected to guard MPEG video quality from packet loss for period of time transmission over the web. as a result of MPEG uses inter-frame secret writing, comparatively little packet loss rates in informatics transmission will dramatically cut back the standard of the received MPEG video. within the projected high-priority protection (HiPP) technique, the MPEG video stream is split into high- and low-priority partitions, employing a technique the same as MPEG-2 knowledge partitioning. Overhead resilient knowledge for the MPEG video stream is made by applying forward error correction secret writing to solely the high-priority portion of the video stream. The high- and low-priority knowledge, and resilient knowledge, ar sent over one channel, employing a packetization technique that maximizes resistance to burst losses, whereas minimizing delay and overhead. as a result of the projected technique has low delay and doesn't need re-transmission, it's compatible for interactive and multicast applications. Simulations were performed examination the advance in video quality victimisation the HiPP technique, victimisation experimental net packet loss traces with loss rates within the vary of 0–8.5%. Overhead resiliency knowledge rates of 1/3, 12.5%, 25%, and 37.5% were studied, with completely different compositions of the overhead knowledge for the twenty fifth and thirty seven.5% overhead rates, in a shot to search out the “best” composition of the overhead knowledge. within the presence of packet loss, the received video quality, as lived by PSNR and therefore the Negsob measure, was considerably improved once the HiPP technique was applied.

4) stratified coded vs. multiple description coded video over erring networks

AUTHORS: Y.-C. Lee, J. Kim, Y. Altunbasak, and R. M. Mersereau

Layered (LC) and multiple description secret writing (MDC) are projected as supply secret writing techniques that ar sturdy to channel errors for video transmission. LC and MDC have similar characteristics: they each generate multiple sub-bitstreams, and it's permissible to drop some portion of the info from the sub-bitstreams throughout transmission for each ways. However, {they ar|they're} {different|totally completely different|completely different} within the sense that the sub-bitstreams for LC have different levels of importance whereas all sub-bitstreams for MDC are equally vital. Since these 2 cryptography techniques have similar properties, some performance comparisons between LC and MDC have recently been reportable. However, these studies ar still not conclusive as a result of many eventualities haven't been fastidiously thought of. moreover, they need been performed in several environments. during this paper, we tend to additional investigate the error-resilience capabilities of those 2 cryptography techniques through intensive experimentation. though a number of our conclusions believe those within the literature, we tend to believe that this paper provides the foremost comprehensive performance comparison nevertheless between LC and MDC.

5) stratified secret writing vs. multiple descriptions for video streaming over multiple ways

AUTHORS: J. Chakareski, S. Han, and B. Girod

In this paper, we tend to examine the performance of specific implementations of multiple description secret writing and of stratified secret writing for video streaming over erring packet switched networks. we tend to compare their performance victimisation completely different transmission schemes with and while not network path diversity. it's shown that, given specific implementations, there's an outsized variation in relative performance between multiple description secret writing and stratified secret writing betting on the utilized transmission theme. For eventualities wherever the packet transmission schedules are often optimized in a very rate-distortion sense, stratified secret writing provides a stronger performance. The converse is true for eventualities wherever the packet schedules aren't rate-distortion optimized.

A. *Existing System*

A decisive for determining the outcome affecting the video streaming services is that the protection of the bit stream from unauthorized use, duplica-tion and distribution.One of the foremost standard approaches to stop undesirable contents distribution to unauthorized users is the technology of Digital Rights Management. Most DRM techni-ques use scientific discipline or digital watermark techniques. However, this sort of approaches don't have any vital impact on distribution of contents, decrypted or improved at the user-side by approved however malicious users.

Disadvantages of Existing System

Moreover, distribution is technically now not tough by victimization peer-to-peer (P2P) streaming software package . Hence,streaming traffic could also be leaked to P2P networks.

B. *Prposed System*

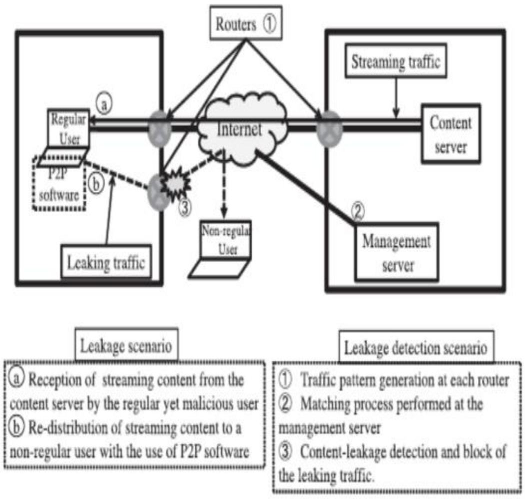
In this paper, we have a tendency to target the outlawed distribution of streaming content by a certified user to external networks. the prevailing proposals monitor info obtained at completely different nodes within the middle of the streaming path. The retrieved info ar accustomed generate traffic patterns that seem as distinctive wave per content, similar to a fingerprint.

Advantages of Proposed system

These technologies enhance the distribution of any style of info over the net .

The pattern generation method performed in standard strategies.

C. *SystemArchitecture*


Routers ①
Streaming traffic
ⓐ
Regular User
Internet
Content server
P2P software
ⓑ
③
②
Non-regular User
Leaking traffic
Management server
Leakage scenario
ⓐ Reception of streaming content from the content server by the regular yet malicious user
ⓑ Re-distribution of streaming content to a non-regular user with the use of P2P software
Leakage detection scenario
① Traffic pattern generation at each router
② Matching process performed at the management server
③ Content-leakage detection and block of the leaking traffic.

D. *Domain Introduction*

a) Networking: Networking is that the word essentially concerning computers and their property. it's fairly often utilized in the globe of computers and their use in numerous connections. The term networking implies the link between 2 or a lot of computers and their devices, with the very important purpose of sharing the information hold on within the computers, with one another. The networks between the computing devices ar quite common currently thanks to the launch of varied hardware and pc code that aid in creating the activity way more convenient to create and use.

b) How it works: When computers communicate on a network, they transport knowledge packets while not knowing if anyone is listening. Computers in a very network all have a association to the network which is termed to be connected to a network bus. What one laptop sends out can reach all the opposite computers on the native network. For the various computers to be ready to distinguish between one another, each laptop encompasses a distinctive ID referred to as MAC-address (Media Access management Address). This address isn't solely distinctive on your network however distinctive for all devices that may be connected to a network. The MAC-address is tied to the hardware and has nothing to try to to with IP-addresses. Since all laptops on the network receives everything that's sent out from all different computers the MAC-addresses is primarily utilized by the computers to filtrate incoming network traffic that's addressed to the individual computer.When a laptop communicates with another laptop on the network, it sends out each the opposite computers MAC-address and therefore the MAC-address of its own. therein approach the receiving laptop won't solely acknowledge that this packet is on behalf of me however additionally, United Nations agency sent this knowledge packet thus a come response are often sent to the sender.

On AN local area network network as delineated here, all computers hear all network traffic since they're connected to an equivalent bus. This network structure is termed multi-drop.One drawback with this network structure is that once you have, let say 10 (10) computers on a network and that they communicate ofttimes and attributable to that they sends out there knowledge packets willy-nilly, collisions occur once 2 or a lot of computers sends knowledge at an equivalent time. once that happens knowledge gets corrupted and needs to be resent. On a network that's serious loaded even the resent packets impinge on different packets and have to be compelled to be resent once more. actually this presently becomes a information measure drawback. If many computers communicate with one another at high speed they will not be ready to utilize quite twenty fifth of the whole network information measure since the remainder of the information measure is employed for resending antecedently corrupted packets. The thanks to minimize this drawback is to use network switches

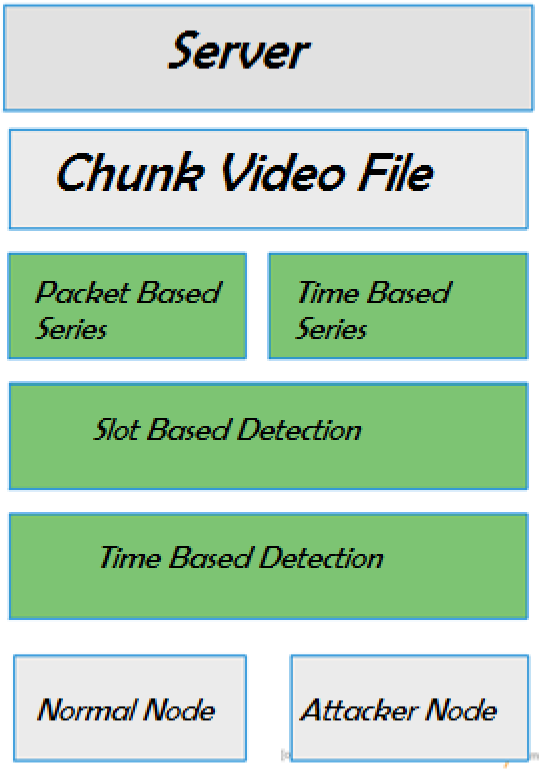
c) .Characteristics of Network:

- Peer-to-peer networks
- Server Based networks

d) Advantages:

- Easy Sharing of Hardware
- Easy sharing of software
- Robustness
- Security
- Abilities of Sharing Data And Information

III. FIGURES



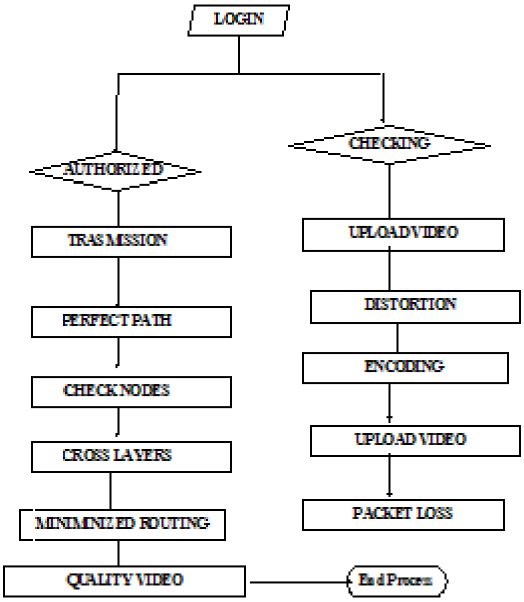


Fig: Data Flow Diagram

IV. CONCLUSION

The content discharge detection system supported the very fact that every streaming content incorporates a distinctive itinerary is AN innovative answer to stop criminal distribution of contents by an everyday, nevertheless malicious user. although 3 typical standard strategies, namely, T-TRAT, P-TRAT, and DP-TRAT, show lustiness to delay, disturbance or loss of packets, the performance of detection decreases with substantial variation of video lengths. This paper makes an attempt to resolve these problems by introducing a dynamic discharge detection theme. Moreover, during this paper, we tend to investigate the performance of the planned methodology below a true network surroundings with videos of various lengths. The planned methodology permits versatile and correct streaming content discharge detection freelance of the length of the streaming content, which boosts secured and sure content delivery.

V. References

[1] O. Adeyinka, "Analysis of IPSec VPNs Performance during a transmission setting," 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. hand-picked Areas Comm., vol. 16, no. 4, pp. 573-586, May 1998.

[4] M. Barni and F. Bartolini, "Data concealment for Fighting Piracy," IEEE Signal process Magazine, vol. 21, no. 2, pp. 28-39, Mar. 2004.

[5] K. Su, D. Kundur, and D. Hatzinakos, "Statistical physical property for Collusion-Resistant Digital Video Watermarking," IEEE Trans. Multimedia, vol. 7, no. 1, pp. 43-51, Feb. 2005.

[6] E. Diehl and T. Furon, "Watermark: Closing the Analog Hole," Proc. IEEE Int'l Conf. client physical science, pp. 52-53, 2003.

[7] 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.

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

[9] M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Traitor Tracing Technology of Streaming Contents Delivery victimization path in Wired/Wireless Environments," Proc. IEEE international Telecomm. Conf., pp. 1-5, Nov./Dec. 2006.

[10] K. Matsuda, H. Nakayama, and N. Kato, "A Study on Streaming Video Detection victimization Dynamic path," IEICE Trans. Comm., vol. J19-B, no. 2, pp. 166-176, 2010.

[11] A. Asano, H. Nishiyama, and N. Kato, "The impact of Packet rearrangement and Encrypted Traffic on Streaming Content run Detection (Invited Paper)," Proc. Int'l Conf. laptop Comm. Networks (ICCCN '10), pp. 1-6, Aug. 2010.tp://networks.cs.ucr.edu/testbed