ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 124-129 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp22.pdf

TRAFFIC SUCCESSION CAPACITY PROVINCE OUTFLOW FOR ATTACHED CONTENT DISTRIBUTION NETWORKS

Miss. K.Spandana[1], Asso.Prof.Sowjanya[2]

[1]*II M.Tech. - II Sem., Dept. of CSE, St. Ann's College of Engineering. & Technology. Chirala, Andhra Pradesh -,523 187 INDIA,*
Sumam.koti@gmail.com

[2]*Asso.Professor &Head , Dept. of CSE, St. Ann's College of Engg. & Tech., Chirala, A. P, INDIA*
drharinicse@gmail.com

ABSTRACT

Multimedia streaming applications and services unit of measurement turning into trendy in recent a year, that's why issue of trustworthy video delivery to forestall the undesirable content outflow becomes necessary. The quality Systems self-addressed this issue by proposing ways that during which supported observation of streamed traffic throughout the network. The duty of maintaining high detection accuracy where as managing traffic variation among the network is completed by ancient system. However it'll decrease the detection performance to the various variation of length of the detection video. To overcoming this issue we have a tendency to tend to face live proposing a very distinctive outflow detection of content theme that's sturdy to the variation of the length of the video.

We have a tendency to focus on overcoming this issue by proposing a completely distinctive in the content-leakage detection theme that is durable to the variation of length of the video. Ready the length of assorted videos, we've got an inclination to tend to substantiate a relation between video length to be compared and put together the similarity between the videos that unit of measure compared. When analysis of the applying, the effectiveness of our planned theme is evaluated in terms of variation of video length, variation in delays, packet and knowledge loss.

INTRODUCTION

In recent years, with the quick development of broadband technologies and so the advancement of high-speed wired/wireless networks, the popularity of amount of your time video streaming applications and services over cyber web has accumulated by leaps and bounds. YouTube and Microsoft Network [2].

(MSN) videos aren't prepared samples of such applications. They serve a colossal population of users from all rounds the planet with varied contents, ranging from daily news feeds to amusement feeds along with music, videos, sports, then forth, by victimization streaming transmission technologies. in addition, amount of your time video streaming communications like internet conference in intra-company networks or via net with Virtual personal Networks (VPNs) area unit being wide deployed in associate degree passing sizable quantity of companies as a strong suggests that of efficiently promoting business activities whereas not additional costs [3]

A crucial concern in video streaming services is that the protection of the bit stream from unauthorized use, duplication and distribution. One in every of the

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 124-129 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp22.pdf

foremost customary approaches to prevent undesirable contents distribution to unauthorized users and/or to protect authors' copyrights is that the Digital Rights Management (DRM) technology. Most DRM techniques use crypto logical or digital watermark techniques. However, this type of approaches haven't got any vital result on re-distribution of contents, decrypted or improved at the user-side by accredited but malicious users. Moreover, distribution is technically not hard by victimization Peer to appear (P2P) streaming package. Hence, streaming traffic may even be leaked to P2P networks.

On the alternative hand, packet filtering by firewall-equipped egress nodes could be an easy resolution to avoid outpouring of streaming contents to external networks. Throughout this resolution, the packet header info (e.g., destination and supply internet Protocol (IP) addresses, protocol kind, and port vary of outgoing traffic) of each streamed packet is inspected. Merely simply just in case the inspected packets don't verify the pre-defined filtering policy [7], they're blocked and born. However, it's troublesome to utterly stop streaming content outpouring by suggests that of packet filtering alone as a results of the packet header info of malicious users could be a few beforehand and may be just spoofed.

During this work, we tend to tend to concentrate on the prohibited re-distribution of streaming content by an accredited user to external networks [8]. The prevailing proposals in monitor information obtained at utterly totally different nodes among the center of the streaming path. The retrieved information area unit accustomed generates traffic patterns that appear as distinctive undulation per content, just like a fingerprint. The generation of pattern does not would like any information on the packet header, and then preserves the user's privacy. Outpouring detection is then performed by scrutiny the generated traffic patterns. However, the existence of videos of varied lengths among the network setting causes a considerable degradation among the outpouring detection performance [12-14]. Thus, developing associate innovative outpouring detection technique durable to the variation of video lengths is, so needed. Throughout this paper, by scrutiny utterly totally different length videos, we tend to tend to verify a relationship between the length of videos to be compared and their similarity. Supported this relationship, we tend to tend to verify decision threshold sanction native correct outpouring detection even in associate setting with utterly totally different length videos. First we tend to tend to depict the drawback of the prevailing theme because of the variation of video length in realistic setting, and then we tend to tend to delineate the planned outpouring detection theme, which we tend to decide its calculation price compared to that of the prevailing theme. We tend to tend to gauge the effectiveness and so the accuracy of the planned theme with relevance utterly totally different length videos, and its strength to network setting changes.

RELATED WORK

I. CONTENTLEAKAGE DETECTION

In this section, we first take a look at a typical video leakage scenario, and we present an overview of existing traffic pattern based leakage detection technologies.

A.Typical video leakage scenario

Due to the recognition of streaming delivery of flicks, development of P2P streaming computer code has attracted a lot of attention. These technologies enhance the distribution of any kind of info over the web. A typical content outflow state of affairs is represented by the subsequent steps as portrayed in Fig. 1. First, an everyday user during a secure network receives streaming content from a content server. Then, with the utilization of a P2P streaming computer code, the regular nevertheless malicious user redistributes the streaming content to a non-regular user outside its network. Such content-leakage is hardly detected or blocked by watermarking and DRM based mostly techniques [15].

A.Leakage detection procedures

Throughout the video streaming method, the changes of the quantity of traffic seem as a novel wave specific to the content. Therefore by watching this

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 124-129 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp22.pdf

info retrieved at completely different nodes within the network, content-leakage is detected.

An overview of the topology of the planned outpouring detection system is shown in Fig. 1. This topology consists of 2 main parts, particularly the route generation engine embedded in every router, and also the route matching engine enforced within the management server. Thus every router will observe its traffic volume and generate route. Meanwhile, the route matching engine computes the similarity between traffic patterns through an identical method, and supported specific criterion, detects contents outpouring. The result's then notified to the target edge router so as to dam leaked traffic [5].

A. Pattern generation algorithm

Here, we tend to describe the route generation method performed in standard ways. Route generation method relies on a either time slot-based formula or an impact on re-distribution of contents, decrypted or rebuilt at the user-side by licensed however malicious users. Moreover, distribution is technically now not troublesome by victimization Peer to see (P2P) streaming code. Hence, streaming traffic could also be leaked to P2P networks.

On the opposite hand, packet filtering by firewall-equipped egress nodes is a straightforward answer to avoid discharge of streaming contents to external networks. During this answer, the packet header info (e.g., destination and supply web Protocol (IP) addresses, protocol kind, and port range of outgoing traffic) of each streamed packet is inspected. Just in case the inspected packets don't verify the pre-defined filtering policy, they're blocked and born. However, it's troublesome to completely stop streaming content discharge by means that of packet filtering alone as a result of the packet header info of malicious users is unspecified beforehand and may be simply spoofed [13] [14].

In this work, we tend to specialize in the amerceable re-distribution of streaming content by a certified user to external networks. The prevailing proposals in monitor info obtained at totally different nodes within the middle of the streaming path. The retrieved info are accustomed generate traffic patterns that seem as distinctive wave per content, a bit like a fingerprint. The generation of route doesn't need any info on the packet header, and so preserves the user's privacy. Discharge detection is then performed by comparison the generated traffic patterns. However, the existence of videos of various lengths within the network surroundings causes a substantial degradation within the discharge detection performance. Thus, developing Associate in nursing innovative discharge detection technique sturdy to the variation of video lengths is, so needed. During this paper, by comparison totally different length videos, we tend to confirm a relationship between the length of videos to be compared and their similarity. Supported this relationship, we tend to confirm call threshold sanctionative correct discharge detection even in Associate in Nursing surroundings with totally different length videos. The rest of the paper is organized as follows. A typical video discharge state of affairs, detection system and procedures are delineating in section II. In section III, initial we tend to depict the downside of the prevailing theme because of the variation of video length in realistic surroundings, then we tend to delineate the planned discharge detection theme, and that we measure its calculation value compared thereto of the prevailing theme. What is more, in section IV, we tend to measure the effectiveness and also the accuracy of the planned theme with relation to totally different length videos, and its hardiness to network surroundings changes [9]. Finally, we tend to conclude this paper packet size-based formula. The route generated is expressed as Associate in Nursing N-dimension vector as follows, packet size-based formula. The route generated is expressed as Associate in Nursing N-dimension vector as follows,$\mathbf{XN=(x1,x2,….xN)}^{T}$**;**

(1) Where xi indicates the volume of the i^{th} chunk, and N is the total number of chunks.

Time slot-based algorithm is a straightforward solution to generate traffic patterns by summing the amount of traffic arrival during a certain period of time, t. In case some packets are delayed, they may be stored over the following slot, xi+1, instead of the primary slot, xi. Therefore, delay and jitter of packets distorts the traffic pattern, and as a consequence, decreases the accuracy in pattern matching.

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 124-129 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp22.pdf

Moreover, time slot-based algorithm is affected by packet loss.

Packet size-based algorithm defines a slot as the summation of amount of arrival traffic until the observation of a certain packet size. These algorithms only make use of the packet arrival order and packet size, therefore is robust to change in environment such as delay and jitter. However, packet size based algorithm shows no robustness to packet loss.

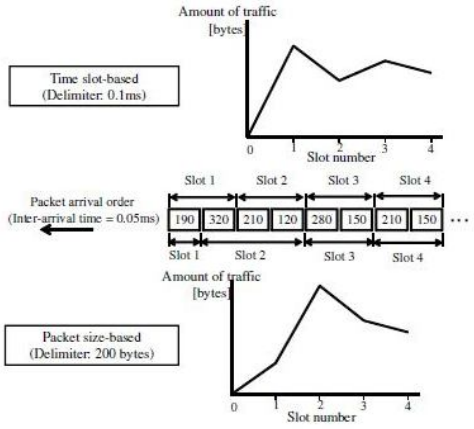


Fig2.
Traffic Pattern generation process

Fig.2. Describes an example of time slot-based generation process and packet size-based generation process. Here, the time-slot, _t is set to 0.1 milliseconds for time slot-based process, while for packet size-based process, slots are generated by summing the amount of arrival traffic until observing a packet of size less than 200 bytes.

A.Pattern matching algorithm

In pattern recognition, the degree of similarity is defined to be the similarity measure between patterns. The server side traffic patterns represents the original traffic pattern and is expressed as XS = (x1; x2; :::; xS)t according to Eq. 1. The user-side traffic pattern is expressed as YU = (y1; y2; :::; yU)t. Here, S and U are number of slots, and the length of the user-side observation is shorter than that of the server-side, i.e., S > U. steps. First, we set a window of size, U, which snips off a partial pattern, XU, from the server-side traffic pattern, XS. Next, we compute the similarity between the partial pattern, XU, and the user-side pattern, YU, (partial similarity). The window is then moved from left to right by one slot. These three steps are repeated until the window reaches the rightmost part of the server-side pattern. Thus, we obtain (S □ U + 1)

Values of similarity. The maximum value is then retrieved and represents the degree of similarity of the compared videos.

a. Leakage detection criterion

The cross correlation matching algorithm is performed on both the traffic patterns generated through time slot based algorithm and those generated through packet size based algorithm. The similarity data obtained from the matching of time slot-based generated traffic patterns are considerably small and their distribution is considered to be normally distributed around zero, since the distribution of cross-correlation coefficient values of two random waveforms is approximated to a normal distribution. Therefore, uses a dynamic decision threshold based on the Chebyshev's inequality, and given by the following equation:

On the other hand, the DP matching algorithm is performed on traffic patterns generated through packet size-based algorithm. Therefore, a fixed predefined value is used as the decision threshold. Whether or not patterns are similar is decided by comparing the distance computed through DP matching with the decision threshold, i.e., the distance less than the threshold indicates that the compared traffic patterns are similar.

I.ENHANCEMENTOFDETECTION TECHNIQUE TO HANDLE VIDEOCONTENTS OF DIFFERENT LENGTHS

Among the conventional methods, DP-TRAT method shows high robustness to packet delay, jitter, and packet loss. However, the existence of videos of different lengths subjected to time variation in real content delivery environment causes DPTRAT's accuracy to decrease. In this section, we take a look

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 124-129 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp22.pdf

At the issue caused by the existence of different length videos in network environments. While focusing on DP-TRAT, we introduce a new threshold determination method based on an exponential approximation, and evaluate the computation cost of both the proposed scheme and an eventual enhancement of the previous scheme.

A.Issue due to different lengths of videos

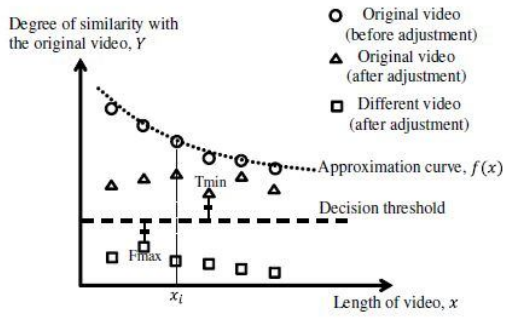
Traffic patterns of streaming videos represent the skeleton carrying their characteristics, and are unique per content. Therefore, the longer the traffic pattern is, the more information on the video it displays. In conventional methods, it is assumed that a certain length of content can always be obtained through the network for all contents. Therefore it is possible to utilize a fixed decision threshold in both PTRAT and DP-TRAT methods. However, there is no such guarantee in actual network environments.

A.Exponentialapproximation-based threshold determination and leakage detection

1)Thresholddetermination process (pre-processing)

Fig 2.0 Determination of the decision threshold for detecting leakage.

Fig. 2 depicts the determination of 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, we perform an exponential approximation of the form



f(x)=exp(α.x+β): (2)

This exponential curve represents the estimation of the degree of similarity with the original video for a certain length x. It is computed based on the least-squares method. Where **α** and **β** are given by Eq. 3 and Eq. 4.

$$\alpha = \frac{n \cdot C - B \cdot D}{n \cdot A - D^2} \quad (3)$$

$$\beta = \frac{A \cdot B - C \cdot D}{n \cdot A - D^2} \quad (4)$$

1)Leakage detection

Before the leakage detection process, we compute the approximation curve based on the original traffic pattern. Then we compare the target traffic pattern to the original traffic pattern, and we adjust the obtained degree of similarity using the approximation curve following Eq. 8, where x is the size of the target traffic pattern. Finally, we compare the adjusted degree of similarity to the decision threshold specific to the original video, and detect whether or not there is a leakage. The problem in comparison of short length videos is then solved, and a flexible and accurate leakage detection method is possible [5].

CONCLUSION

The detection of content discharge system supportedthe very fact that each streaming content encompasses adistinctivepath is an innovative resolutionto forestallsmuggled re-distribution of contents by an everyday, nevertheless malicious user. Three typical standardways, specifically T-TRAT, P-TRAT, DP-TRAT, show strength to delay, information or packet loss, the detection performance decreases with sizeable variation of video lengths.

This paper triesto unravel these problems by introducing a dynamic discharge detection scheme. Moreover, during this paper, we have a tendency to investigate the performance of the plannedmethodologybeneatha true network environment with videos of various lengths. The planned method permitsversatile and correct streaming content leakage detection freelance of the

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 124-129 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp22.pdf

length of the streaming content, which reinforces secured and trusty content delivery.

REFERENCES

1)Y. Chu, S. G. Rao, S. Seshan and H. Zhang, "Enabling conferencing applications on the Internet using an overlay multicast architecture," in Proc. ACM SIGCOM, pp.55-67, California, USA, Aug. 2001.
2)Z. Yang, H. Ma, and J. Zhang, "A dynamic scalable service model for SIP-based video conference," in Proc. 9th International Conference on Computer Supported Cooperative Work in DE.
3)Y. Chu, S. G. Rao, S. Seshan and H. Zhang, "Enabling conferencing applications on the Internet using an overlay multicast architecture," in Proc. ACM SIGCOM, pp. 55-67, California, USA, Aug. 2001.
4)O. Adeyinka, "Analysis of IPSec VPNs Performance in A Multimedia Environment," School of Computing and Technology, University of East London.
5) 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
6)S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications," IEEE J. Sel. Areas Commun., vol.16, no.4, pp.573-586, May 1998.
7)M. Barni and F. Bartolini, "Data hiding for fighting piracy," IEEE Signal Process. Mag., vol.21, no.2, pp.28-39, Mar. 2004.
8)K. Su, D. Kundur, and D. Hatzinakos, "Statistical invisibility for collusion-resistant digital video watermarking," IEEE Trans. Multimedia, vol.7, no.1, pp.43-51, Feb. 2005.
9)E. Diehl and T. Furon, "Watermark: Closing the analog hole," in Proc. IEEE Int. Conf. Consumer Electronics, pp.52-53, 2003.
10)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.
11)E. D. Zwicky, S. Cooper, and D. B. Chapman, "Building Interent Firewalls (2nd ed.)," O'Reilly and Associates, 2000.
12)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," in Proc. IEEE Global Telecommunications Conference, pp.1-5, San Francisco, USA, Nov./Dec. 2006.
13)K. Matsuda, H. Nakayama, and N. Kato, "A Study on Streaming Video Detection using Dynamic Traffic Pattern," IEICE Transactions on Communications (Japanese Edition), vol.J19-B, no.02, 2010.
14)Atsushi Asano, Hiroki Nishiyama, and Nei Kato, "The Effect of Packet Reordering and Encrypted Traffic on Streaming Content Leakage Detection (Invited Paper)," International Conference on Computer Communication Networks 2010 (ICCCN 2010), Zurich, Switzerland, Aug. 2010.
15)S. Amarasing and M. Lertwatechakul, "The Study of Streaming Traffic behavior," KKU Engineering Journal, vol.33, no.5, pp.541-553, Sept.- Oct. 2006.
16)Y. Gotoh, K. Suzuki, T. Yoshihisa, Hideo Taniguchi, and M. Kanazawa, "Evaluation of P2P Streaming Systems for Webcast," 6th International Conference on Digital Information Management.

AUTHORS :

Miss. K Spandana Devi Studying II M.Tech (CSE) in St. Ann's College of Engineering & Technology,Chirala,She completed B.Tech.(CSE) in 2013 in St. Ann's Engineering College, Chirala.

Ms. YALLANTI SOWJANYA KUMARIis presently working as AssociateProfessor, in Department of Computer science & Engineering in St. Ann's College of Engineering and Technology, Chirala. She has 8 Years of Teaching Experience.