An SDN-based Framework for Detection of Illegal Rebroadcasting of Channels in P2PTV

Arash Shaghaghi[1,2], Jaesung Hong[1], Sanjay Jha[1]
[1]School of Computer Science and Engineering, University of New South Wales, Sydney, Australia
[2]National ICT Australia (NICTA)
{arashs, jhong, sanjay}@cse.unsw.edu.au

ABSTRACT

Nowadays, mesh based live P2P streaming systems (P2PTV) is a popular means of streaming audio and video content over the Internet. The main reason being that it can accommodate large amounts of users with low cost compared to dedicated servers, or content distribution network solutions. However, one of the issues and impediments associated with this technology is the rebroadcasting of illegal or inappropriate material. This work presents an early architecture that relies on capabilities provided by Software Defined Networking (SDN) to address this issue. We adaptively partition the outgoing P2PTV traffic and distribute detection across a range of detection nodes, which use some of the existing video identification techniques to detect suspicious content. Moreover, due to processing requirements of vector graphics we suggest an assistive scheme so that controllers can push traffic to other controllers' network and take advantage of available resources under their control. To automate this process in a network we propose an extension to distributed SDN controllers architectures so they can actively cooperate. To the best of our knowledge, there is no work that has studied detection of illegal or inappropriate rebroadcasted stream through P2PTV technology and our proposed scheme is novel.

Categories and Subject Descriptors

C.2.m [**Computer-Communication Networks**]: Miscellaneous

Keywords

P2PTV; Illegal Rebroadcasting; Video Content Identification; Software-Defined Networking; Cooperative Controllers

1. BACKGROUND

1.1 P2PTV

In Peer-to-Peer TV, every viewer contributes to the overall capacity of bandwidth by simultaneously uploading the received content to other users. As soon as a user joins a certain channel, the P2PTV software contacts a tracker server that registers the addresses of peers who are watching, which in turn announces this to viewers with the same interest. Similar to file sharing P2P systems, in mesh based P2P-TV systems the video content is sliced in pieces, called chunks. These are then distributed onto an overlay topology on top of the regular Internet for the distribution of real-time video content. Currently, P2PTV is commonly used to distribute streaming of illegal or inappropriate channels such as copyrighted material [1].

1.2 Video Content Identification

Detecting illegal visual material is directly related to the field of copy detection for images and videos, which only recently has saw a burst of activity. The typical method for detection of such in video is detecting key frames that reflect the whole scenes and applying local descriptor creation to those frames. Detection of illegal material like frames containing child pornography seems to be trivial either through cryptographic hashes to recognize the images or comparing frames with identified copies in a given database. A draw back of hashing methods is that they are fragile to any image processing operation such as a simple re-compression with JPEG. On the other hand, image identification methods such as semantic models or face detection require massive computational complexity for large volume of video content and are prone to significant false alarm rates. An alternative solution is using robust hashing that combines the characteristics of both cryptographic hash and image identification methods. As a matter of fact, solutions such as Eff2 Videntifier [2], Videntifer [3] and [4] have discussed efficient solutions for forensic analysis of video content. These can process large amount of information in a short time and find instances of illegal material such as pirated videos. For example, in the case of Videntifier using a combination of local image descriptors based on SIFT and multidimensional NV-trees it is possible to inspect each hour of a video in 30 seconds with 98.6% successful detection rate.

1.3 Software Defined Networking (SDN)

In SDN, the network intelligence is logically centralized and assigned to a software based controller, control plane, and network devices are reduced to basic packet forwarding devices, referred to as data plane. From an architectural point of view one of the key design axes of SDN control platform is centralised versus distributed architecture. In this paper we are interested to distributed controllers such

VideoNext'14, December 2, 2014, Sydney, Australia
ACM 978-1-4503-3281-1/14/12.
http://dx.doi.org/10.1145/2676652.2683465.

as DISCO [5], and D-SDN [6]. By definition in a distributed architecture, there are multiple controllers each with their own distinctive experience and view of the network. There is currently a new trend as interconnected SDN controllers in distributed architecture [7]. In the case of interconnected controllers, each controller can communicate with others through secure east and westbound channels.

2. THE PROPOSED DETECTION SCHEME

Currently, there is no automatic solution to process streamed video in P2PTV and identify inappropriate or illegal transmission of content. This is an important issue for large and enterprise networks, where bandwidth management and users compliance with their policies is of utmost importance. Therefore, network administrators have a binary approach in managing P2PTV related traffic, to either block it completely or allow it with no control. In this work we propose leveraging SDN technology to adaptively slice and distribute a copy of P2PTV traffic into a Deep Packet Inspection (DPI) layer. In other words, a load balancing application on top of the controller distributes the traffic among deep packet inspectors. Considering that the amount of processing associated with each chunk is limited, deep packet inspectors will perform inspection at line-rate in most cases. However, we understand that with wide adoption of P2PTV the amount of traffic could reach an unprecedented rate. Therefore, we propose an extension to interconnected SDN controllers so that they could share video inspection resources dynamically, when processing exceeds their constraints. To achieve this an extra module is added to each controller, which allows live communication about resource availability and facilitates cooperative decision making among controllers for load balancing.

2.1 Detection System

2.1.1 P2PTV traffic detector and load splitter

This module is essentially an SDN application running on a controller such as NOX [8]. It has two main functionalities, which are detection of P2PTV traffic and balancing the load among deep packet inspectors that are accessible to it as a separate subsystem in the network. As the video content is sliced and packet size distribution of P2PTV applications is dynamic, detection of this type of traffic is not straightforward. For example, [10] compares different types of detection methods in terms of success rate and efficiency. The P2PTV traffic detector will employ state of the art algorithms such as [9] that uses application level signatures to detect this type fo traffic. The task of network load splitter is then to logically partition P2PTV traffic and create flow rules to forward a copy of all packets of each slice to a detector node in DPI layer.

2.1.2 Deep Packet Inspection Layer

The deep packet inspection layer is constitute of a central logic, detection nodes and a decision making module. The central logic is responsible for resource management and has a northbound channel to communicate with load splitter and a southbound to interact with detection nodes. Detection nodes are virtual machines that are optimized for video content identification, specifically in regard to GPU requirements. Among existing solutions in the literature, we believe Videntifier could be an excellent candidate for our scheme. Videntifier requires limited processing power, has a high precision and it uses efficient algorithm in sampling key frames of a video for analysis. However, we slightly change its implementation in this case. The client is the detection node that receives PP2PTV traffic chunks for processing. The fingerprints extracted by each detector are then sent to a central Videntifier database server hosted by Eff2 Technologies, which interoperates with similar database servers in other networks. Finally, once the central logic at DPI layer receives a relatively appropriate number of detection outcomes for a set of P2PTV traffic chunks it decides whether to flag it as suspicious or illegal material.

2.2 Cooperative Scheme

We propose an extension to distributed SDN controllers architectures and to exploit the very recent advances in east and westbound connection between them to setup an actively cooperating scheme for load management. Unlike existing distributed SDN controller solutions such as [5] or [6], our scheme does not have a master-slave approach relying on a centralized controller. Instead, controllers are defined as interactive entities who are responsible for their assigned resources and make decisions either independently or cooperatively. The primary reason behind this change is introducing a flexible resource sharing solution for the proposed DPI layer through adaptive reprogramming of the network to manage flows. Moreover, the cooperative scheme could be then extended so that controllers within neighbouring networks redirect specific type of P2PTV application traffic to the controller that employs the most adequate detection system respectively. To implement the cooperative scheme we use an Agent Module (AM) that runs as an application on top of each controller. AM interacts with all the components of detection system and considers the resources available for controller. It also receives updates about the status of neighbouring controllers and makes decisions on how the cooperation should occur.

2.3 Future Work

Currently, some of the well-known P2PTV applications use encrypted traffic whether for all of the communication or stages of it. This is, however, not the case for all P2PTV applications due to performance overheads and Quality of Service (QoS). We will therefore investigate solutions for encrypted services as part of our ongoing research. In theory, our proposed scheme could be applied to any non-encrypted traffic and enable processing of video content identification at line-rate. Therefore, our next step is delivering a prove of concept implementation for our detection systems and evaluate performance overheads. As there are no implementations of interconnected controllers and this is an essential requirement for our proposed cooperative scheme, we are now developing an open API for controllers, which allows secure and efficient transmission of data between controllers.

3. REFERENCES

[1] Seetoo, C.H., 2007. Can Peer-to-Peer Internet Broadcast Technology Give Fans Another Chance-Peer-to-Peer Streaming Technology and Its Impact. U. Ill. JL Tech. & Pol'y, 369.

[2] Dadason, K., Lejsek, H., Ásmundsson, F., Jonsson, B., and Amsaleg, L., 2007. Videntifier: identifying pirated

videos in real-time. In Proceedings of the 15th international conference on Multimedia ACM, 471-472.

[3] Ásmundsson, F.H., Lejsek, H., Dadason, K., Jonsson, B., and Amsaleg, L., 2009. Videntifier forensic: robust and efficient detection of illegal multimedia. In Proceedings of the 17th ACM international conference on Multimedia ACM, 999-1000.

[4] Yannikos, Y., Ashraf, N., Steinebach, M., and Winter, C., 2013. Automating Video File Carving and Content Identification. In Advances in Digital Forensics IX Springer, 195-212.

[5] Phemius, K., Bouet, M., and Leguay, J., 2013. DISCO: Distributed multi-domain SDN controllers. arXiv preprint arXiv:1308.6138.

[6] Santos, M.A.S., Astuto, B.N., obraczka, K., turletti, T., deoliveria, B.T., and Margi, C.B., 2014. Decentralizing SDN's Control Plane. In IEEE Local Computer Networks (LCN).

[7] The Internet Engineering Task Force, The case for SDNi: SDN Controller Interconnection, Available at: http://www.ietf.org/proceedings/84/slides/slides-84-sdnrg-5.pdf, Last checked: 18 October 2014.

[8] Tavakoli, A., Casado, M., Koponen, T., and Shenker, S., 2009. Applying NOX to the Datacenter. In HotNets.

[9] Cascarano, N., Risso, F., Este, A., Gringoli, F., Salgarelli, L., Finamore, A., and Mellia, M., 2010. Comparing P2PTV traffic classifiers. In Communications (ICC), 2010 IEEE International Conference on IEEE, 1-6.

[10] De Carvalho, D.A.M., 2009. Towards the detection of encrypted peer-to-peer file Sharing Traffic and peer-to-peer TV traffic using deep packet inspection methods. University of Beira Interior-Covilhã, Portugal.

[11] Jin, L., Xin, Z., Xiao-Liang, Z., and Hui, W., 2010. Using packet size distribution to identify P2P-TV traffic. In Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2010 International Conference on IEEE, 150-155.