World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:13, No:11, 2019

Internet Optimization by Negotiating Traffic Times

Carlos Gonzalez

***Abstract*—**This paper describes a system to optimize the use of the internet by clients requiring downloading of videos at peak hours. The system consists of a web server belonging to a provider of video contents, a provider of internet communications and a software application running on a client's computer. The client using the application software will communicate to the video provider a list of the client's future video demands. The video provider calculates which videos are going to be more in demand for download in the immediate future, and proceeds to request the internet provider the most optimal hours to do the downloading. The times of the downloading will be sent to the application software, which will use the information of pre-established hours negotiated between the video provider and the internet provider to download those videos. The videos will be saved in a special protected section of the user's hard disk, which will only be accessed by the application software in the client's computer. When the client is ready to see a video, the application will search the list of current existent videos in the area of the hard disk; if it does exist, it will use this video directly without the need for internet access. We found that the best way to optimize the download traffic of videos is by negotiation between the internet communication provider and the video content provider.

***Keywords*—**Internet optimization, video download, future demands, secure storage.

I. Introduction

WITH the advent of companies that provide video content through the World Wide Web (WWW) like Netflix, the demand for bandwidth in the network has increased, mainly to some hours in which most users require bandwidth to download and see their selected videos. This has resulted in internet providers being forced to utilize most of their bandwidth at those peak hours to satisfy the needs of customers downloading videos at peak hours. There has been many works trying to solve this problem; for example, the objective of Wang's [1] invention is to provide an improved method to code documents for their distribution to selected receptors, also supports the transfer of the rights of decoding the document. This is a good option to provide security in the transmission of information, but it does not address a key point like the optimization of traffic.

Sakhartov [2] describes a system to generate interactive video contents. Once the video is selected, this video is associated with a series of commercial information related to it. Again, this patent does not mention any form of optimizing the traffic. On the other hand, we have the work of Harrang [3], in which he teaches a computational method and software modules for the handling of pre-loading of video based on an estimate of the client's future requirements, and a decrement in the use of the internet at peak hours by the user. Unfortunately, the elements that know about the best hours in which the downloading should happen are the internet connection providers, and this important factor is not considered in this patent.

This paper presents a method which will allow the optimization of the bandwidth demand at peak hours. This methodology proposes that the downloading of video content be negotiated between the internet connection providers and the providers of video content. This video content provider will base its needs in the future demands from its clients. These future needs will be calculated on previous user demands, and future projected demands for the customers.

Carlos Gonzalez is with the Universidad Autonoma de Coahuila, Arteaga Mexico (e-mail:gonzalezc757@gmail.com).

II. Methodology

The methodology presented here is for a system to optimize internet traffic when downloading of video content. Fig. 1 shows a system comprised of three modules: 1) a module that represents the video contents provider, 2) a module representing the provider of internet connection (i.e. Internet Service Provider) and, 3) the module representing the final consumer of the video. These three modules communicate with each other using the internet. The communication between the video content providers (1) and the provider of internet connection (2) is represented by communication line 4. On the other hand, the communication between the video contents provider and the final consumer of the video is done through the internet connection utilizing the communications line 4 and line 5.

The final consumer of the video (Fig. 2 #3) is a user computer that could support different operating systems like Microsoft Windows, Mac OS, Google Chrome, Linux, Unix, Android, etc. Fig. 2 shows the final consumer of video. This computer has two modules to handle videos. The Software for Video Contents (Fig. 2 #6) (SVC) is a software provided by the video content provider to the customer when this customer acquires the provider's services, and a storage area, which is an area, separated inside the users' computer where all the pre-load videos will be stored and is called Storage of Pre-Load Video (Fig. 2 #7) (SPLV). This storage area will be accessible only through the SVC, where each video is doubly protected by a secret password and encryption. The SVC will be designed with special techniques used in the creation of self-protected software. These techniques include primarily the use of obfuscation for software programming [4]-[11]. It will also include techniques for the detection of the user [12]-[16], including the type of user and the threat that this user represents, and the action to take for every scenario.

The user through the SVC will provide the system a list of future demands of videos, and will be sent (Fig. 2 #11) to the video contents provider. This future demand will be based on the previous use of the user, and the actual contents in the

user's SPLV. When the user wants to see a video, he makes his request to the SVC; this module will check if the petitions is preloaded in the SPLV (Fig. 2 #7), and will be sent (Fig. 2 #8) to the SVC where it will be authenticated and decrypted for the user use. On the other hand, if the requested video is not in the SPLV, then a requirement (Fig. 2 #13) will be sent for the download of this video at this time. When the video content provider receives this requirement, it proceeds to send the user the requested video (Fig. 2 #12). The SVC receives from the video content provider, a timetable to do the downloading (Fig. 2 #15). At the pre-established times, the SVC requests a download from the video server (Fig. 2 #14). The videos that will be pre-downloaded (Fig. 2 #10) are sent to the final video consumer.

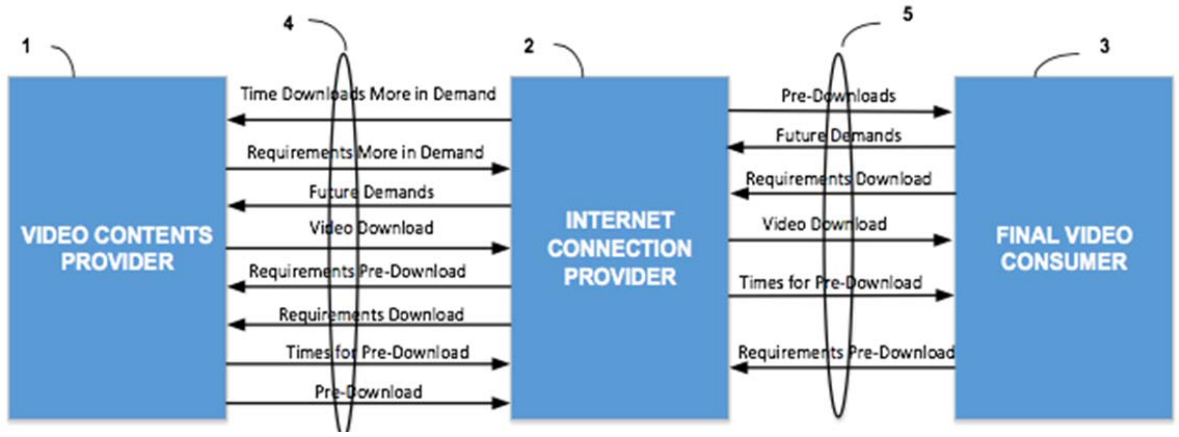

Fig. 1 Providers and Consumer

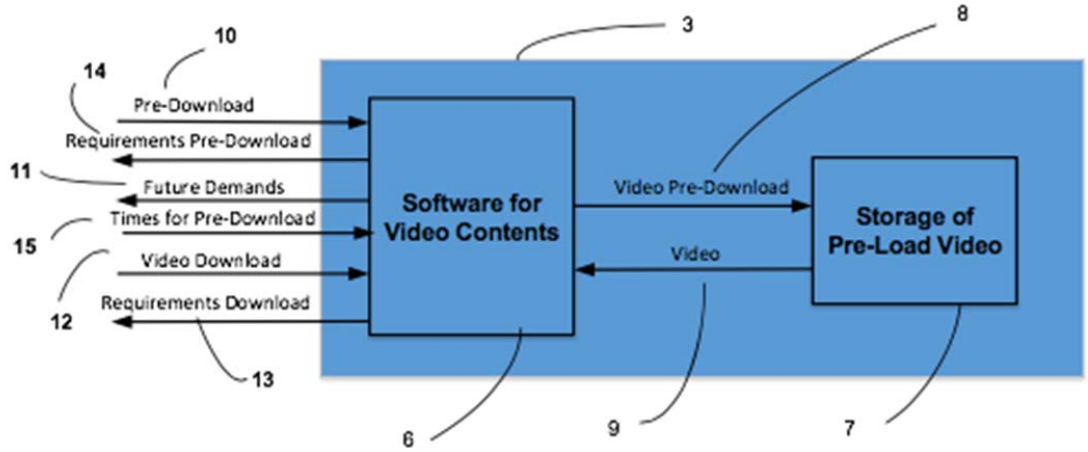

Fig. 2 Final Video Consumer

The videos that are going to be pre-loaded (Fig. 2 #10) are send to the final video consumer (Fig. 2 #3) and are received by the SVC (Fig. 2 #6), which will authenticate and make sure they are properly encrypted and then pass them over (Fig. 2 #8) to the SPLV (Fig. 2 #7).

The service providers shown in Fig. 3, are the providers of internet connection (Fig. 3 #2), and the provider of video content (Fig. 3 #1). The provider of the video content is comprised of two modules to provide this service. The first module is a server (a computer connected to a network) of video content (Fig. 3 #18). This server is connected directly to the internet and is in charge of providing service to customers that require video content. This server receives from the customer, via the internet, three types of information: 1) a requirement for a download of a video (Fig. 3 #13), 2) a requirement of a pre-download of video (Fig. 3 #14), and 3) the list of future demands of customer (Fig. 3 #11). With the requirement of video download, the server proceeds to send the customer the requested video (Fig. 3 #12). The list of future demands of the customer (Fig. 3 # 11) is used by the server to construct a list of videos with more demands and sends (Fig. 3 #20) it to the second module of this video content provider, which is the negotiator of times to make a pre-download (Fig. 3 #22) (NTPD). This module is in charge of negotiating with the provider of internet connection 2 at what times it will be best to make the pre-load of videos. This information of requirements of more demand (Fig. 3 #16) is sent to the Internet Connection Provider, to wait for the times (Fig. 3 #17) to make the preloading of the videos to his clients and to optimize the use of the connection. Once the NTPD has this information, it will pass it to the server as information for the pre-downloading (Fig. 3 #21). The server uses this

information to send the final client a time for the pre-downloading (Fig. 3 #15) that will be used to request from the server the pre-downloading at the indicated times and proceed to do the pre-loading of videos to the customers (Fig. 2 #10).

It should be noted that if the system consists of more than one internet connection provider, the video content provider will have to negotiate downloading times with each of them separately.

The Internet Connection Provider (Fig. 3 #2), conceptually is comprised of two modules. One will be the Negotiator of Times to make a Pre-Download (Fig. 3 #23), and the module that provides the internet connection (Fig. 3 #19). When the negotiator module receives from the provider of video content, the information of the more in demand videos (Fig. 3 #16), this information and the information of user demands that are not clients of the Provider of Video Content will be used to plan which will be the most beneficial time to do these downloads (Fig. 3 #17), and then optimize the internet bandwidth. It is expected that most of the time, these hours will be in the early hours of the day when internet usage is at its lowest point. In any case, the one that knows and can predict the behavior of the internet usage is the provider of the internet provider.

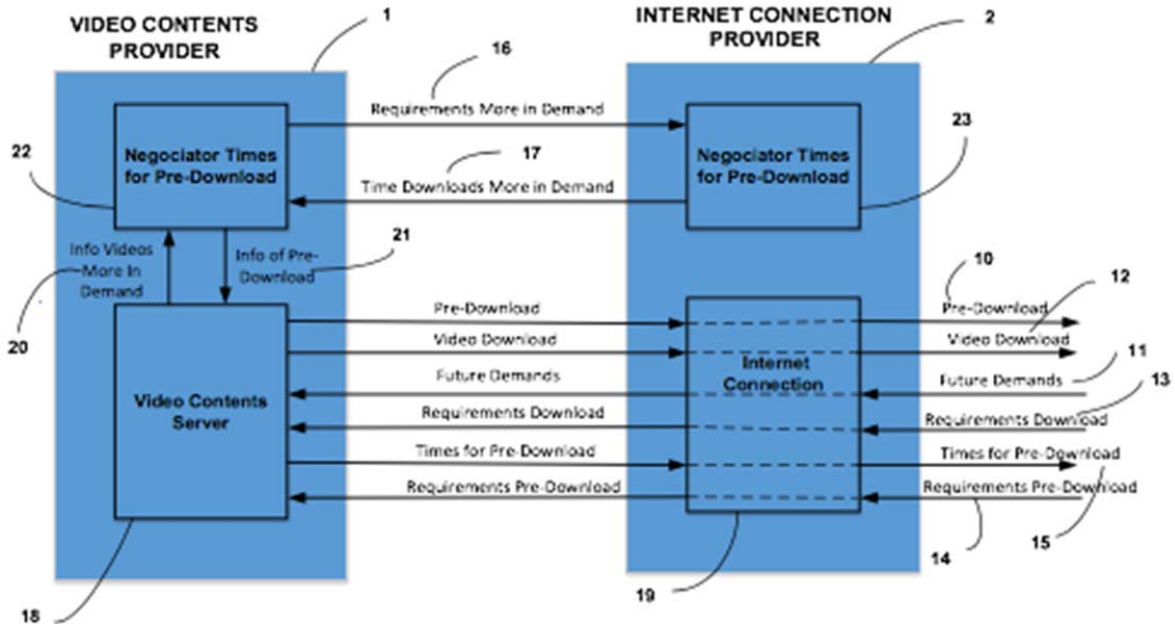

Fig. 3 Providers Communication

III. Conclusions

The main contribution of this paper is the explicit use of negotiations between the providers of video content and the providers of internet connection to obtain the most beneficial time to download the videos for the final consumer of the video content. Since the entity that knows the most about the user future requirements for video downloads is the provider of video content, and the one that know more about the internet traffic is the provider of the internet connection, negotiations among them will generate optimal use of the internet for the downloading of video content.

As stated before, the major findings of this research are that optimization based only on the user profile and decisions done at the local user level, as has been proposed in many studies, is not complete without input from the video provider and the Internet Service Provider.

Another important contribution is the use of obfuscation techniques to design the software to handle the storage space inside the client's computer. Finally, a new innovative use of a software engineering technique mentioned in this paper is the user detection for the self-protected software used in the handling of the transaction for the separated storage space.

References

[1] Wang in "Sistema y método para distribución de documentos.", España patent ES2265826 T3, March-01-2007
[2] Sakhartov et al., "Systems and methods for generating interactive video content", USA Patent 8,166,500 , Apr-24-2012
[3] Harrang; Jeffrey et al., "Pre-Delivery Of Content To A User Device", U.S. Pub No. 2015/0039601 A 1, Feb-05-2015
[4] Amit Sahai and Brent Waters. (2013). "How to Use Indistinguishability Obfuscation: Deniable Encryption, and More", http://eprint.iacr.org/2013/454.pdf
[5] Amit Sahai, et al., (2013). "Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits", http://eprint.iacr.org/ 2013/451.pdf
[6] Aucsmith D., (1996). "Tamper Resistant Software: An Implementation", Proc. 1st International Information Hiding Workshop (IHW), Cambridge, U.K. Springer LNCS 1174, pp. 317-333.
[7] Barak B., O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, K. Yang, (1997). "On the Impossibility of Obfuscating Programs", pp. 1–18, Advances in Cryptology– Crypto 2001, Springer LNCS 2139 (2001).
[8] Collberg C., C. Thomborson, D. Low, (1997) "A Taxonomy of Obfuscating Transformations", Technical Report 148, Dept. Computer Science, University of Auckland (July 1997).
[9] Collberg C., C. Thomborson, D. Low, (1998). "Manufacturing Cheap, Resilient, and Stealthy Opaque Constructs", Proc. Symp. Principles of Programming Languages (POPL'98), Jan. 1998
[10] Kevin A. Roundy and Barton P. Miller, (2011). "Binary-Code Obfuscations in Prevalent Packer Tools", http://ftp.cs.wisc.edu/pub/

paradyn/papers/Roundy12Packers.pdf, September 2011
[11] Toshio Ogiso, Sakabe Yusuke, Soshi Masakazu, Miyaji Atsuko. (2003). "Software Obfuscation on a Theoretical Basis and its Implementation", IEEE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, January 2003, 176-186.
[12] Denning, Dorothy E., "An Intrusion Detection Model," Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131.
[13] Scarfone, Karen; Mell, Peter. "Guide to Intrusion Detection and Prevention Systems (IDPS)". Computer Security Resource Center (National Institute of Standards and Technology) (800–94) (February 2007).
[14] Mukherjee B., Heberlein L.T, Levitt K. N.," Network Intrusion Detection", IEEE Network May 1994
[15] Scarfone Karen, Mell Peter., "Guide to Intrusion Detection and Prevention Systems (IDPS)", Computer Security Resource Center (National Institute of Standards and Technology), February 2007
[16] Gonzalez C., "User Detection in Military Software", The Journal of Cyber Security and Information Systems, submitted Nov 2018.