Circumvent Traffic Shaping Using Virtual Wireless Clients in IEEE 802.11 Wireless Local Area Network

Omar Nakhila[1] and Cliff Zou[2]

***Abstract*— Accessing the Internet through Wi-Fi networks offers an inexpensive alternative for offloading data from mobile broadband connections. Businesses such as fast food restaurants, coffee shops, hotels, and airports, provide complimentary Internet access to their customers through Wi-Fi networks. Clients can connect to the Wi-Fi hotspot using different wireless devices. However, network administrators may apply traffic shaping to control the wireless client's upload and download data rates. Such limitation is used to avoid overloading the hotspot, thus providing fair bandwidth allocation. Also, it allows for the collection of money from the client in order to have access to a faster Internet service. In this paper, we present a new technique to avoid bandwidth limitation imposed by Wi-Fi hotspots. The proposed method creates multiple virtual wireless clients using only one physical wireless interface card. Each virtual wireless client emulates a standalone wireless device. The combination of the individual bandwidth of each virtual wireless client results in an increase of the total bandwidth gained by the attacker. Our proposed technique was implemented and evaluated in a real-life environment with an increase in data rate up to 16 folds.**

***Index Terms*— Wi-Fi Security; Wi-Fi hotspot; Virtual Wireless Client; Wi-Fi Traffic Shaping;**

I. Introduction

Staying connected to the Internet has become a priority in our daily routines. At the same time, the increase in Internet data traffic, due to the wide spread of high-definition multimedia, has pushed us to search for high-speed Internet access [1]. Clients can use cellular service to have high-speed Internet access through their mobile data connection. Although mobile broadband is convenient, it is also expensive and may fluctuate based on the wireless coverage area. On the other hand, businesses such as fast-food restaurants, coffee shops, hotels, and airports, may provide complementarity Internet access to their clients through the use of Wi-Fi hotspots. Using these Wi-Fi hotspots to access the Internet offers a budget friendly alternative to mobile data connection [2].

Wi-Fi hotspots allow clients to simultaneously connect different wireless devices to the Internet [3]. However, network administrators may impose wireless bandwidth limitations on the wireless devices accessing the Internet through these Wi-Fi hotspots [4][5][6]. Each wireless device will be assigned a certain download and upload speed to access the Internet. The reason behind these limitations is to prevent customers from abusing the complimentary Internet service, to provide fair bandwidth allocation, and to make the customer pay to have a faster Internet connection.

Different commercial software are available to increase the client Internet connection speed. For example, an increase in the Internet downloading speed can be achieved by initiating different connections simultaneously to the same file on the Internet [7][8]. The summation of all connection's speed will result in a faster file download speed. However, bandwidth limitations are implemented at the data link and network layer which make it difficult for these tools to take advantage of the multiple data connections. The bandwidth controller will detect that all of these connections are initiated from one single wireless client and thus reduce the speed of all the connections to a single one.

However, an attacker may circumvent the traffic shaping policy applied by the wireless network administrators by using virtual wireless clients technique. Although the virtual wireless clients technique was developed to improve the wireless network performance and privacy [9], in our work, it is used as a tool to attack wireless network infrastructure [10][11].

In this paper, we improve wireless network security by:

- Presenting a network vulnerability to avoid Wi-Fi hotspot bandwidth limitation by using multiple Virtual Wireless Clients (VWCs). Using only one wireless network interface card, an attacker can create multiple virtual wireless clients. Each VWC emulates a standalone wireless device. The VWCs start multiple connections to a remote file on the Internet.
- The bandwidth allocated to each VWC is separate from other VWCs which allows the attacker to overload the hotspot using only one physical wireless interface card.
- The proposed technique was implemented and evaluated in real-life scenarios using off the shelf devices.

The paper is organized in the following order: Section II discusses related works. The design of the traffic shape attack is presented in Section III. Then, the proposed attack evaluation is shown in Sections IV. Discussion, limitation and future work are presented in Section V. Finally, our conclusions are presented in section VI.

II. Related Work

A high-speed connection is an attractive option when it comes to accessing the Internet. One of the convenient methods to connect to the Internet is to use the cellular data connection. The client can also use her mobile as a Wi-Fi hotspot and share the data connection with other users. However, most cellular companies charge a lot of money

[1] Department of Electrical and Computer Engineering, University of Central Florida, omar_hachum at knights.ucf.edu

[2] Department of Computer Science, University of Central Florida, czou at cs.ucf.edu

978-1-5386-0595-0/17/$31.00 ©2017 IEEE

TABLE I: Software used in our testbed evaluation. Software were installed on Linux O.S except IDM which was installed on Windows O.S.

Protocol	Transfer Software	File Server	Port
TFTP	tftp	Xinetd	69
FTP	ftp	VsFTPd	20,21
HTTP	IDM	Apache2	80
HTTP	VWC (Proposed)	Apache2	80

when it comes to accessing the Internet; while other cellular companies even limit the amount of data being downloaded or uploaded to/from the Internet.

On the other hand, businesses such as fast food restaurants, coffee shops, hotels, and airports may provide complimentary connection to the Internet through public Wi-Fi hotspots. These public Wi-Fi hotspots may impose traffic shaping to limit the bandwidth of their wireless clients. Such a limitation features can be freely available in many commercial wireless devices through Guest Wi-Fi option [12][13].

Wireless clients can use different techniques to increase the Internet connection speed. For example, the wireless client throughput can be increased by using UDP-based Data Transfer Protocol (UDT) [14]. The UDT technique employs UDP protocol to transfer files instead of using TCP protocol. The removal of the connection-oriented protocol overhead will reduce the amount of control traffic and increase the actual data traffic. However, the connection will be still throttled by the bandwidth limiter since the protocol does not change the physical and logical address of the wireless client. Furthermore, UDT is designed to be used with high-speed networks.

Another method that can be used by the wireless client is to employ a commercial software such as Internet Download Manage (IDM) [8]. IDM accelerates the file transfer up to five times by initiating multiple connections to the same file on the Internet [7]. Each connection starts from different parts of the file. The total download speed equals to the summation of all the connection's speeds to the file. However, this technique is also limited by the bandwidth controller since the wireless client can still be identified by her IP and MAC address.

Increasing the Internet connection speed can be also achieved when the wireless client uses both, the mobile data and the Wi-Fi hotspot connections simultaneously. In [15], clients can combine both Internet connections using a proxy server. Data request will be sent to a proxy server that is used to load balance the download/upload speeds between the two network connections on the wireless client. However, this technique uses the mobile data connection, and it also limited by the speed of the hotspot bandwidth limiter.

In this paper, we present an attack to bypass the bandwidth limitation used in public Wi-Fi hotspot by using virtual wireless clients technique.

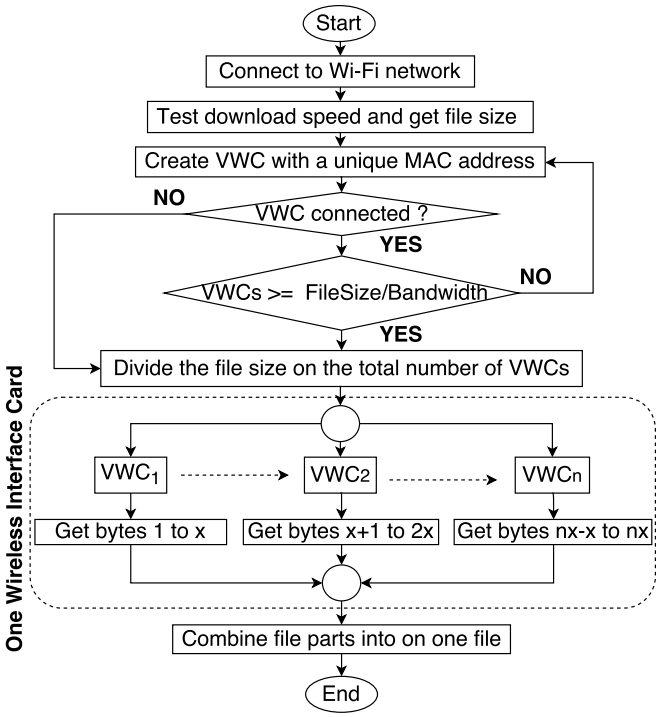

Fig. 1: Proposed attack design on Wi-Fi hotspot traffic shaping using Virtual Wireless Clients.

III. Proposed Traffic Shaping Attack

A. Assumption

Our proposed attack targets Wi-Fi hotspots that imposed a bandwidth limitation on their wireless clients. Wireless network administrators avoid network overload by assigning a dedicated bandwidth to each wireless client. Based on the complexity of the wireless network design, a network administrator may use IP and MAC addresses to identify wireless clients. This type of bandwidth limitation is common in public Wi-Fi hotspots such as fast food restaurant, coffee shops, hotels, and airports.

B. Attack scenarios

The attacker can use the VWCs technique to pass the Wi-Fi hotspot traffic shaping in many scenarios. For example, whenever an application wants to access the Internet, a VWC is created and assigned to that application. In a web browser, each opened tab can be assigned to a separate VWC. However, some VWCs may still suffer from bandwidth limitation when they exceed the bandwidth allocated to them. For example, when an open browser tab requests to download a file, the VWC assigned to that browser tab can not exceed the bandwidth limitation allocated to it.

Another scenario is when multiple VWCs work together to download a single file from the Internet. Each VWC starts downloading the single file from a different starting byte location. Some file servers allow clients to request a file from a specific byte number [7]. In this case, the VWCs will start downloading the file simultaneously from different locations. The parts received by the VWCs will be combined at the

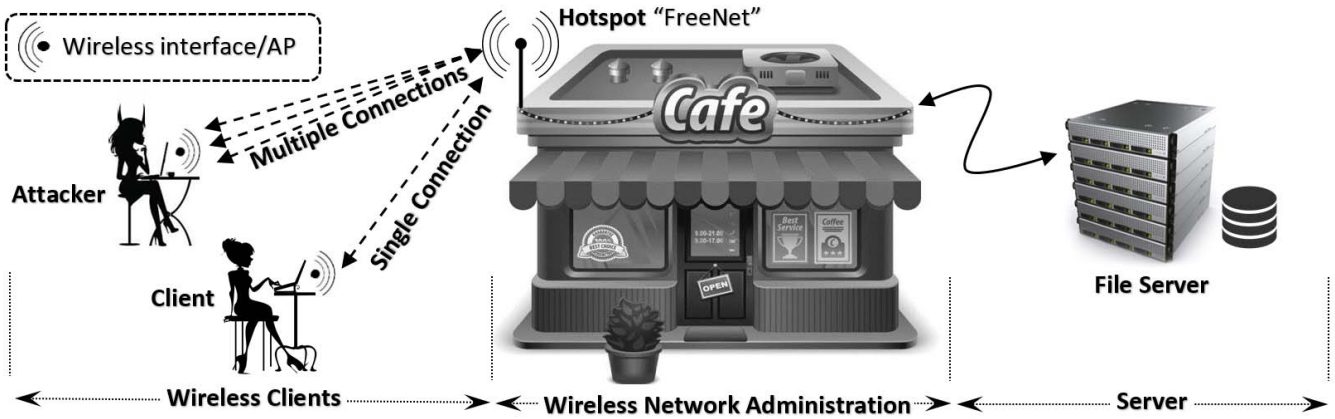

Fig. 2: Proposed attack testbed set up. The attacker and the client used Laptops with TPE-NUSBDB wireless network interface card to connect to the wireless network. Dlink DIR-890L was used as a hotspot and bandwidth controller. We used a Linux based workstation to create the File Server.

client's device. However, this scenario may not work when the server does not support byte-serving technique.

Finally, an attacker can set up a special server on the Internet to overcome the limitations in the previous scenarios. The attacker communicates directly with the special server while the special server retrieve the online resources (such as a file) from other servers on the Internet. The special server can obtain online resources faster than the VWCs, because the Internet connection speed between the special server and other servers, is not restricted by the bandwidth limitation such as the one between the attacker and the special server. After that, the special server can divide the online resource into multiple parts and send them to the attacker's VWCs.

In this paper, we focused on avoiding the traffic shaping technique used by the hotspot when a client downloads a specific file on the Internet.

C. Design

The proposed attack is based on the Virtual Wireless Clients technique. Using only one wireless network interface card, the attacker creates multiple Virtual Wireless Clients that each will have a unique IP and MAC address. All VWCs connect simultaneously to the Wi-Fi hotspot to access the Internet and start downloading the file as shown in figure 1.

First, the attacker connects to the Wi-Fi hotspot and test the bandwidth assigned to her by the wireless network administrator. The attacker can calculate the bandwidth limitation by measuring the time needed to download a small file from the Internet. After that, the attacker gets the size of the actual file that will be download using the VWCs.

The maximum number of VWCs that will be used to download the file is based on the file size and the bandwidth allocation as shown in equation 1.

$$NumberofVWCs = \frac{FileSize}{AllocatedBandwidth} \quad (1)$$

Since the hotspot may limit the number of wireless clients to connect to it, our proposed attack keeps testing if the newly created VWC is able to reach the Internet.

After the attacker finishes creating the VWCs, each VWC starts requesting different parts of the file using a byte serving technique [7]. Since the number of the created VWC may be less than the number from equation 1, each VWC request part size equals to equation 2.

$$RequestingPartSize(x) = \frac{FileSize}{TotalVWCs} \quad (2)$$

After the VWCs finishes downloading all file parts, the software combines them into one.

D. Implementation

We have developed a software written in C language with the help of Loss Of Radio CONnectivity (LORCON2) library [16]. LORCON2 is an open source library used to allow the wireless client to inject crafted wireless frames and at the same time capture wireless traffic on the operating wireless channel.

First, the software authenticates and associates to the AP. After that, using DHCP protocol, the software obtains the network configuration from the DHCP server. Finally, using DNS and HTTP protocol, the software access the Internet. The developed software repeats the previous procedure for each created virtual wireless client.

IV. Evaluation

Our proposed attack on the Wi-Fi hotspot bandwidth controller was evaluated in a real-life testbed set up shown in figure 2. The testbed set up consisted of three main parts, wireless clients, wireless network administration and file server.

The wireless client's side contains two laptops: one represents a regular wireless client and the other one resembles an attacker. We installed our proposed software on the attacker's laptop, while on the other laptop, we installed a different file transfer software such IDM. Both laptops connect to the wireless network side and start downloading files from the file server side. In this way, we can compare our software downloading speed with others. Table I illustrates software used in our evaluation.

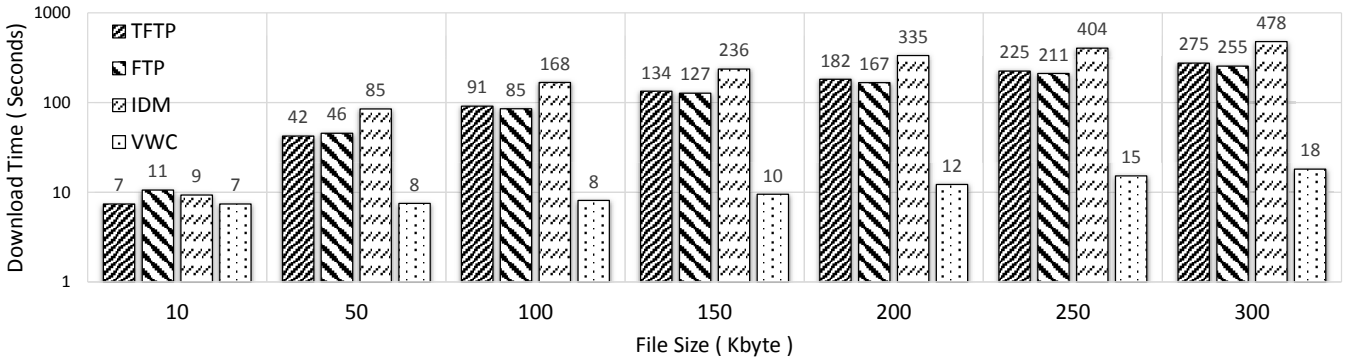

Fig. 3: The time needed to download different files from the file server using the software in Table I. Y-axis is log-10 scale.

On the wireless network administration side, we used D-Link DIR-890L with DD-WRT firmware to create the Wi-Fi hotspot. The hotspot assigned a specific download and upload speed to each wireless client using Quality Of Service (QoS) option. QoS use different packet scheduler algorithms such as Hierarchical Token Bucket (HTB) [17]. Any Wireless client that connects to the hotspot will be allocated 10 Kbytes data rate limit for upload and another 10 Kbyte for download. This uplink and downlink speed can be set to any arbitrary number, however, having a higher bandwidth limitation in our evaluation might produce inconsistent results since other factors such as channel congestion may affect the download/upload speed which is not part of the bandwidth limitation policies.

On the Server side, we created a standard file server. We installed TFTP, FTP and HTTP services on a Linux-based workstation. These services are standard file transfer protocols used to transfer data on the Internet [18]. The server response to TFTP on UDP port 69, FTP on TCP port 20 and 21 and HTTP on TCP port 80. The file server held different file size to be downloaded from the laptops at the wireless client side. All the traffic from the wireless client side to the file server side pass through the wireless network.

Our proposed attack took advantage of the byte serving technique used in HTTP/1.1 protocol. The wireless client can request a specific part of a file to be downloaded. If the requested range is valid, the server starts sending the file. Each virtual wireless client starts downloading different portions of the file simultaneously.

We tested the time needed for the regular wireless client and the attacker to download different files from the file server using TFTP, FTP, and HTTP. Each test was carried separately. We used the default TFTP client software in Linux O.S on the wireless client laptop while Xinetd software was used on the server side. VsFTPd was used on the server side to provide FTP protocol service, while the default Linux FTP software was used on the wireless client laptop. IDM software was used on the wireless client laptop to download the files using HTTP protocol while Apache server was used on the file server side. Finally, our proposed VWC software was installed on the attacker laptop and utilized to download files from the Apache server on the file server. Table I illustrate the client/server software used in our testbed evaluation.

The files on the server side were 10 to 300 Kbytes in size with 50 Kbytes increment. The link speed between the file server and the Wi-Fi hotspot was 100 Mbytes/second. However, the download and the upload speed between the wireless client side and the wireless network administration side was set to 10 Kbits/second. We started downloading each file using the software shown in Table I.

Using our VWC technique, we set the number of virtual wireless clients based on equation 1. For example, for 10 Kbytes file size, we only created one VWC. Since the bandwidth limit was set to 10 Kbit/second, the time needed to download the file was 7.5 seconds. All other methods used to download the 10 Kbytes file size on the regular wireless client were able to finish in about 10 to 7 seconds. This is because the actual file size is 80 Kbits which need 80 Kbits / 10 Kbit/seconds = 8 seconds to finish downloading.

We further increased the file size to 50 Kbytes. Since the file size is 50 Kbytes, our proposed technique created 5 VWC based on equation 1. In our proposed method, the time needed to download the 50 Kbytes was similar to the time needed to download the 10 Kbytes file. On the other hand, the methods used by the regular wireless client to download the 50 Kbytes file size increased by five folds to the time needed to download the 10 Kbytes file. Figure 3 illustrates the measured time to finish downloading different file sizes on both the attacker and the regular wireless client laptop.

However, during the increase of the number of VWCs, we noticed that the attacker started to receive a constant data rate from the Wi-Fi hotspot. When the number of VWCs were more than 20, the wireless connection to the hotspots started to timeout and drop as shown in figure 4. By using our software, the attacker was able to gain almost 16 folds bandwidth increase, while all other transfer methods had a constant download speed.

V. DISCUSSION, LIMITATION AND FUTURE WORK

In this paper, we illustrated a practical attack on the traffic shaping protection used in public Wi-Fi network. We tested our attack effectiveness by comparing it with different file transfer methods. By using VWCs technique,

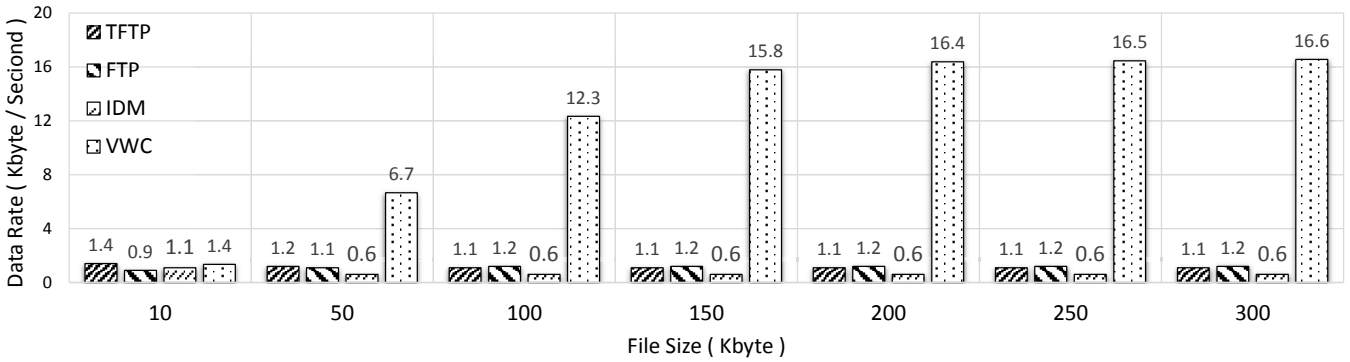

Fig. 4: Comparison between download data rate for each software (Table I) used in our testbed evaluation.

an attacker can bypass bandwidth limitation imposed by network administrators. The attacker creates multiple virtual wireless clients and connects them simultaneously to the Wi-Fi hotspot. The VWCs technique increased the wireless link speed up to 16 folds. However, the following limitation may affect the performance of such an attack.

First, our proposed attack is based on downloading files from servers that support a byte-serving technique, which is available in the HTTP/1.1 standard. Our attack will not work when the file server is using FTP or TFPT since both protocols do not support such a feature. In this case, the attacker can implement a proxy server on the Internet. When the attacker requests a resource from the Internet, the request will be sent to the proxy server. Since the connection speed between the proxy server and the Internet resource is fast, the proxy server acquires the resource, divides it and sends it to the attacker's VWCs. On the attacker's end, all the parts of the resource will be combined. In this case, the attacker can download files even when the file server does not support a byte serving technique.

Second, the wireless network administrator that provides credentials to their wireless clients may impose bandwidth limitations using the wireless client's username and password instead of using the IP and MAC address of the wireless client. In this case, our proposed attack will not work. However, this requires the network administrator to set up a more complex wireless network infrastructure and assign and give each wireless client a unique username and password.

Finally, increasing the number of VWCs will increase the traffic on the wireless channel that can affect the download/upload speed. Also, certain APs limit the number of the wireless clients that can connect to it simultaneously.

VI. Conclusion

Network administrators may impose traffic shaping techniques to protect their wireless network from being overloaded and offer fair bandwidth allocation. Also, they may require the client to pay in order to increase their Internet network connection speed. However, using a VWC technique, an attacker can bypass such a limitation by creating multiple virtual wireless clients using only one physical wireless interface card. Each VWC connects to the wireless network as a standalone wireless client and reserve a separate bandwidth. The total bandwidth that is being used by the attacker, in this case, equals to the summation of all the VWCs bandwidths. Our proposed technique was implemented and evaluated using off the shelf devices. The result shows that the attacker can speed the Internet connection up to 16 folds compared to other file transfer methods.

Acknowledgements

This work is supported by the National Science Foundation under grant SaTC-EDU-1723587.

References

[1] Cisco Inc. *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016 to 2021*, 2017.
[2] L. Qiu, H. Rui, and A. Whinston. When cellular capacity meets wifi hotspots: A smart auction system for mobile data offloading. In *2015 48th Hawaii International Conference on System Sciences*, pages 4898–4907, Jan 2015.
[3] M. Seufert, T. Griepentrog, V. Burger, and T. Hofeld. A simple wifi hotspot model for cities. *IEEE Communications Letters*, 20(2):384–387, Feb 2016.
[4] D. J. Henry. *CCNP Wireless (642-732 CUWSS)*. Cisco Press.
[5] Wifi hotspot for single & chain coffee shop and cafes. Technical report, 2017.
[6] James Eades. Recognising the challenges and trends faced in technology within the hotel industry. Technical report, 2017.
[7] Roy T. Fielding, Yves Lafon, and Julian Reschke. Hypertext Transfer Protocol (HTTP/1.1): Range Requests. RFC 7233, June 2014.
[8] Tonec Inc. *Internet Download Manager*, 2016.
[9] F. Zhang, W. He, and X. Liu. Defending against traffic analysis in wireless networks through traffic reshaping. In *2011 31st International Conference on Distributed Computing Systems*, pages 593–602, 2011.
[10] O. Nakhila, A. Attiah, Y. Jinz, and C. Zou. Parallel active dictionary attack on wpa2-psk wi-fi networks. In *Military Communications Conference, MILCOM 2015 - 2015 IEEE*, pages 665–670, Oct 2015.
[11] O. Nakhila and C. Zou. Parallel active dictionary attack on ieee 802.11 enterprise networks. In *MILCOM 2016 - 2016 IEEE Military Communications Conference*, pages 265–270, Nov 2016.
[12] Cisco. Captive Portal Configuration Guide. Technical report, 2014.
[13] Unifi enterprise wifi system. Technical report, 2017.
[14] Se-young Yu, Nevil Brownlee, and Aniket Mahanti. Performance and fairness issues in big data transfers. In *Proceedings of the 2014 CoNEXT on Student Workshop*, CoNEXT Student Workshop '14, pages 9–11, New York, NY, USA, 2014. ACM.
[15] Alex Gizis. *Speedify Software*, 2017.
[16] Joshua Wright and Michael Kershaw. Lorcon2 project, 2016.
[17] J. L. Valenzuela, A. Monleon, I. San Esteban, M. Portoles, and O. Sallent. A hierarchical token bucket algorithm to enhance qos in ieee 802.11: proposal, implementation and evaluation. In *IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004*, volume 4, pages 2659–2662 Vol. 4, Sept 2004.
[18] Behrouz Forouzan. *Data communications and networking*. McGraw-Hill Higher Education, New York, 2007.