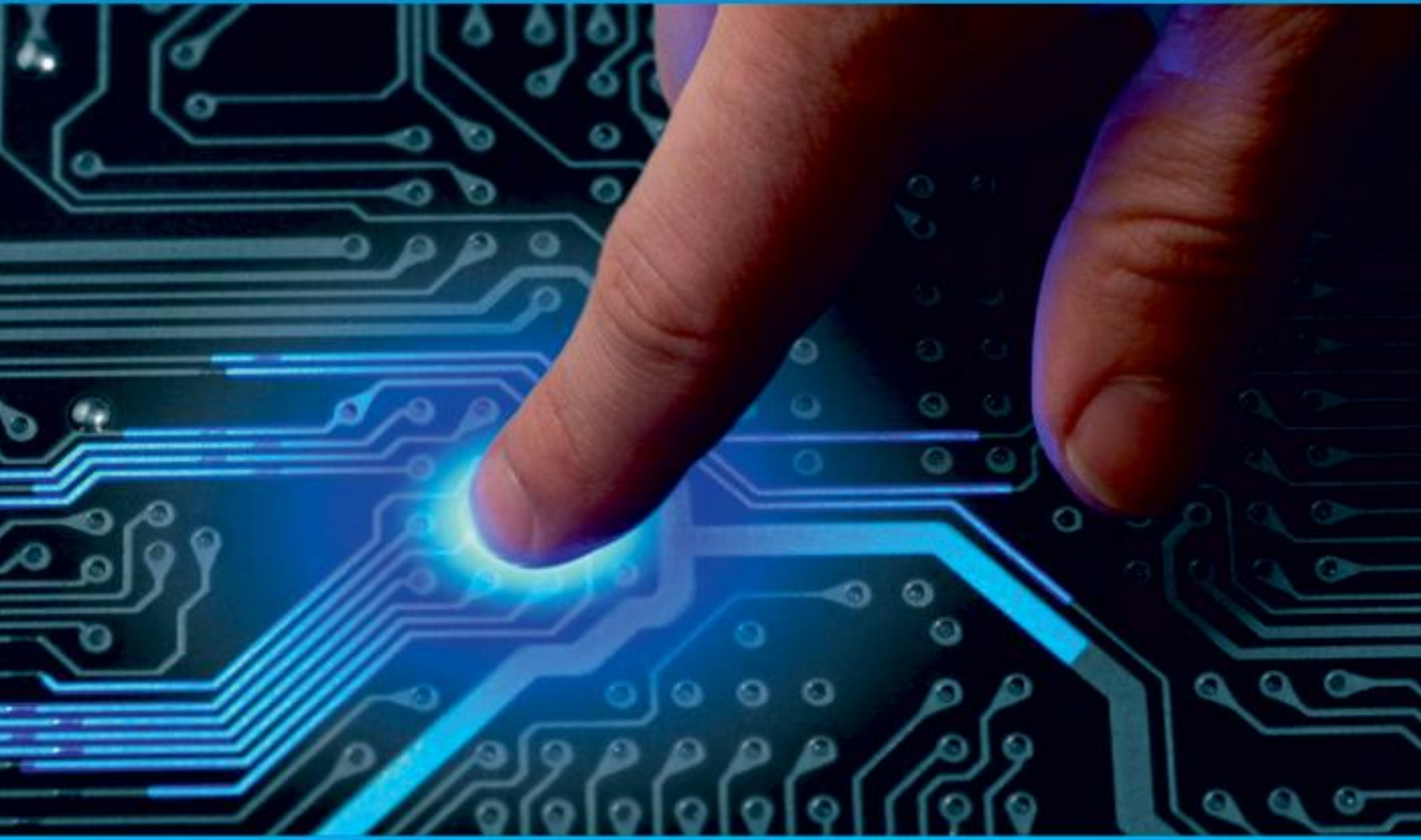
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105251 |

DNS BASED AD BLOCKING

Prof. Balasaheb Gite [1], Chhabildas Yewale[2], Bhushan Parkhi[3], Om Chandgude[4], Akshay Jedhe[5]

Department of Computer Engineering, ISBM College of Engineering, Savitribai Phule Pune University, Nande, Pune, India

Head of the Department, Department of Computer Engineering, ISBM College of Engineering, Savitribai Phule Pune University, Nande, Pune, India

ABSTRACT: This paper presents the evaluation of AdBlock technique implementation for enterprise network environment. This study has presented the impact of web browsing activities where it is the most active traffic where is consumed the highest inbound bandwidth usage in enterprise network environment. We canconclude that DNS AdBlock is the best solution for enterprise network environment in term of blocking advertisement compare to extension adblock. Adblock technique also reduce network data request by comparing front-end solution (browser extension AdBlock) at client web browser and networks level adblock.

This number increased when industries are moving to cloud web-based consumption. However, industries such as educational sector, web browsing traffic is one of connectivity that enterprises network should be investing to support openness and heavy traffic from educational users.

I. INTRODUCTION

Internet browsing is becoming essential part of everyday life often as it often used to gatherinformation. At somehow, web contents delivered to the end user browser with online web advertisements (ads). Daily onlineactivity of thousands of users in one network environment give an impact of online advertisement which can increase the traffic as well as increase bandwidth consumption. As World WideWeb (WWW) makes it more intelligent, the implantation of online web ads in website is one of themarketing strategies [1]. Web technologies are currently moving from Web 2.0 to Web 3.0, online ads contents are becoming one of the elements and it playa big role in web-eco-system [2]. A new semantic format of embedding online ads which would encourage large publishers to add them to their web sites [3]. Besides, online web ads became the basic revenue source for webpage publishers, where they just simply copy the code provided by the ad network provider then paste it into their HTML file. Moreover, with Web 4.0 and Web 5.0; online ads and e-commerce innovations are alreadyunder way [4].

It is a network-level advertisement and internet tracker blocking application which acts as a DNS sink-hole which is intended for use on a private network. When the webpage is being loaded it makes requests to fetchthe required data and Ads together from a separate server. The website has only control over the server thatsendsthe data but has no control over the Ads being displayed.

The system works on the network level and hence it doesn't require any client software or special setup for devices in thenetwork. It makes it possible to block Ads on any device,such as smart TV's that do not allow any modifications. It comes with a Web interface that offers a central place to view and monitor statistics.The web interface can be accessed with any device with a browser within the network. But for network admins, AdGuard can also be used as a network monitoring tool as it can record allDNS queries sent to it and hence it is possible toanalyze and review traffic. This can be particularly helpful during any network investigation and it is also possible for AdGuard to increase network speed. This paper mainly highlights the use of Adguard and the procedure to use it effectively as a DNS on the network.

II. LITERATURE SURVEY

Adblock Plus [13] is an extension that allows the user to improve the web experience. It is available for almost all popularbrowsers. The system is mostly used by masses who don't understand technology. It is a great tool for public networks although it fails to offer network wide protection in a private network. The system doesn't work at the network level and therefore the Ads arefetched by the system in turn consuming system resources andnetwork bandwidth. Although the popularity of the Adblock plus system grew due to its ease of use. However, a major concern is its lack of protecting the privacy of the user as the Ads are fetchedbut just not displayed.

Furthermore, such ad blockers top the list of most popular Firefox extensions, with at least 18M installs [14]that fail in providing privacy.

Other systems that work on the network level like Alternate DNS [15] that is a DNS server which is capable of achievingthe same results to the proposed system but as the DNS server is owned by a third party it allows for monitoring of the DNS requestsbeing made. Ad-away[16] is another such system that works on the network level on a smartphone and uses a private DNS server but lacks ease of use and installation. It requires special root permissions from the system that a typical user won't be able to provide.It provides Ad blocking thatcan be considered private but it only blocks Ads on the device on which it is installed.

III. METHODOLOGY

In this research, the two major types of variables are independent and dependent variables been identified. An independent variable is a variable that affect the dependent variable while dependent variableis the variable a researcher is interested in. The components of variables are shown in Figure 1.

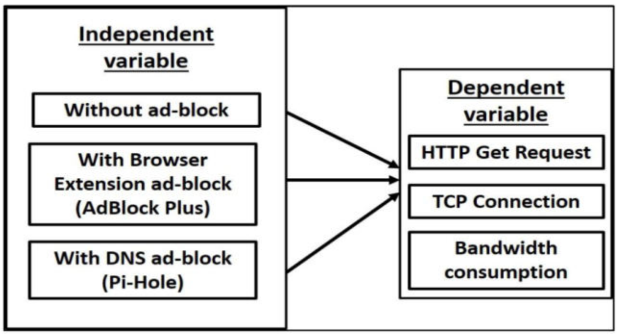


Figure 1. Experimental variables

In this research, there are three independent variables that been manipulated which are network without AdBlock (Scenario 1), network with browser extension AdBlock (Scenario 2), and network withDNS AdBlock (Scenario 3). From all independent component, there are three dependant areas that been investigate which are HTTP “get” request, TCP connection and bandwidth consumption.

Measurement Framework

The framework that been used for this study is similar with previous research conducted by [15] where they used it to investigate the amount of data generated by advertisements when browsing as shownin Figure 2.

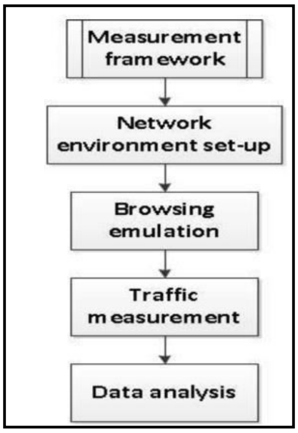


Figure 2. Experimental design approach

Activities conducted in this experiment when we used network packet data to investigate the amountof data generated by advertisements when browsing. This experiment needs to set-up a network environment whereit will be tested with three scenarios as mention before. Web browsing emulation is conducted in each client PC for each scenario. Data collection of the web browsing traffic is measured using packet sniffing program "Wireshark". Further discussion for each steps are explained in next sub-topics.

Network Environment Set-Up

Figure 3 shows the network environment set-up for this study. There are three types of scenarios where the network configured without AdBlock for Scenario 1, Scenario 2 with browser extension and with DNS AdBlock for Scenario 3.

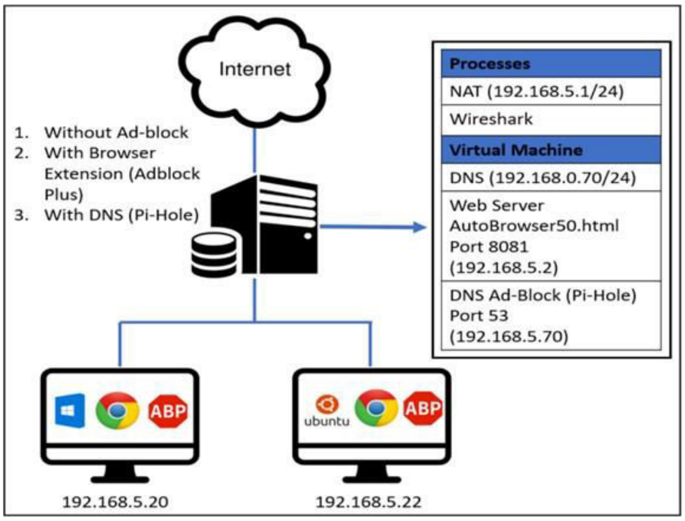


Figure 3. Testing architecture

To simulate the network environment, an isolate network it setup using network address translation (NAT) and this study set-up a network which client PCs connected to the switch and the all PCs will be configured as static IP. Virtual machine installs with Debian operating system to run AutoBrowse at Apache server port 8081. Network traffic is captured using Wireshark software.

In Scenario 1, normal DNS server is implemented as DNS forwarder to same upstream DNS (GoogleDNS) to give a fair and consistent measurement of test traffic in network without AdBlock. In

Scenario 2, AdBlock Plus is implemented in chrome web browser and it point to the same DNS as in Scenario 1. While in Scenario 3, client DNS is pointed to Pi-hole as it future have the ability to perform DNS forwarder together with Ads Blocking.

Web Browsing Emulation

In this reserach, we adapted the mimic surfing using AutoBrowse program written by [17]. This program is in JavaScript and runs on the PCs web browser that retrieves a given set of URLs. There are fifty (50) lists of URLs that has been identified that needed to be loaded from Malaysia and other country website. In order to set up a consistent concurrent request from client web browser, this reserach is modified by adding a new function "gettime()" in AutoBrowse and run it in Apache server. An experimental test timeis set at AutoBrowse source code by modifying the parameters shown in Table 1. Therefore, all PCs are requested for AutoBrowse and retrieve it with the current time in Apache server. All the URLs are loaded for each of the scenario.

Table 1. Gettime () Description

Paramete	Descriptions
Value1	Hours start
Value2	Minutes start
Value3	Seconds start

Traffic Measurement

In this reserach, we decided to use the packet sniffing program Wireshark to capture all traffic from each scenario. Since all data passes through NAT, Wireshark can simply measure data that is being exchanged only for the network. In scenario 1 and 2, all client PC is pointed to local DNS 192.168.0.70. Thus, those two scenarios have the same network flow and forward to same upstream DNS server. While in scenario 3, all client PC is pointed to 192.168.5.70 local DNS configured with Pi-Hole and the same upstream DNS as in scenario 1 and 2. All traffic from each IP address is investigated in Wireshark in to filtering the traffic. Wireshark is filtered the traffic according to the rules.

According to [9], to allow them to have uniform base of comparison across all the controls and all the subsequence they conducted the test one a single day. Therefore, this research is conducted tests for all scenarios within twenty-four (24) hours. All scenarios have to follow procedure below [17] in order to get thereliable result:

a) DNS queries point to same upstream DNS (GoogleDNS).
b) All web browser request to AutoBrowse and start and end concurrently.
c) Clear web browser cache before every test start.
d) Each scenario must be conducted a 3 times test.

Data Analysis

After capturing traffic from all scenarios, we conducted an offline investigation on the traffic generates from web browsing emulation. For data analysis, this experiment filtered on the IP address of the client PC and Autobrowse programs. This research measured each scenario at least three (3) times to get average result. Compare the results of network traffic from all scenarios and get the number of HTTP get request, TCP connection and bandwidth consumption while implemented the AdBlock

IV. SYSTEM DESIGN

A. System Block Diagram

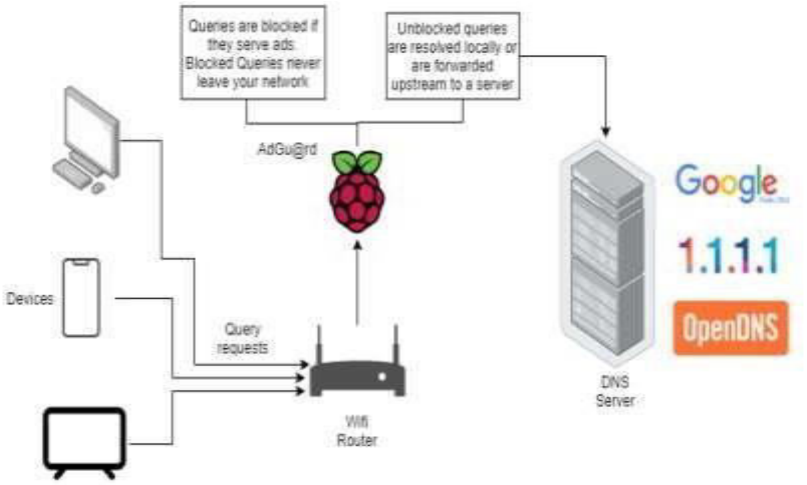

Queries are blocked if they serve ads Blocked Queries never leave your network
Unblocked queries are resolved locally or are forwarded upstream to a server
AdGu@rd
Devices
Query requests
Wifi Router
DNS Server
Google
1.1.1.1
OpenDNS

Fig 1: System Block Diagram

All the devices connected to the router send requests to the router so that devices can display web pages from the Internet.The router uses a DNS (Domain Name System) to translate human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example 192.0.2.44). When using Adguard,
devices that want to find outwhere a server is, the query is first sent to Adguard that acts as a DNS.
If the domain is not an Ad-serving domain (for example, google.com), the associated web page or data is displayed. If Adguard is unable to resolve the domain then a request is sent to an upstream (public) DNS server (OpenDNS, Google DNS). It passes throughthe router and out to the Internet and the webpage is displayed.
If the domain is an ad-serving domain (for example ads.google.com), Adguard responds to your device request and points to an address (0.0.0.0) that has a blank webpage. So in place of the Ad the blank web page is displayed.The request never leaves the network and remains private.

B. Algorithm Based Flow Chart

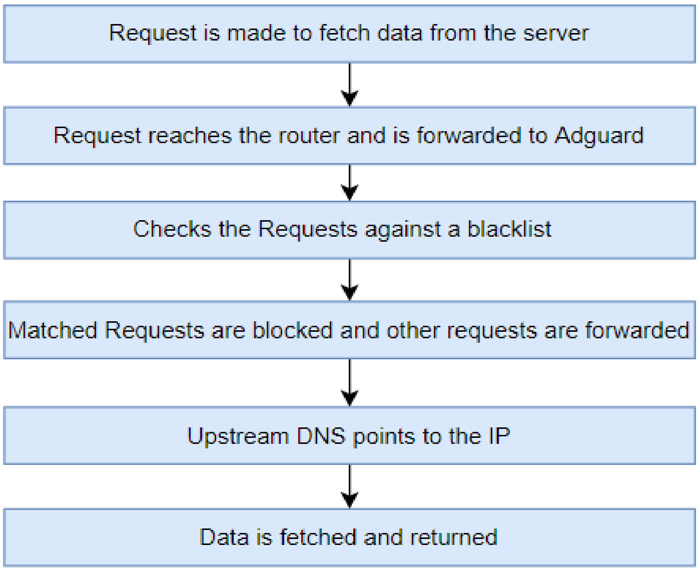

Request is made to fetch data from the server
Request reaches the router and is forwarded to Adguard
Checks the Requests against a blacklist
Matched Requests are blocked and other requests are forwarded
Upstream DNS points to the IP
Data is fetched and returned

Fig 2: FlowChart

When the user visits a website the device makes a request to fetch data from the server. The request is then forwarded to the router. Usually, the router resolves the request by itself or forwards it to an upstream DNSto resolve. Instead of resolving therequest the router forwards the request to Adguard.

Adguard checks the requested domain name against a blacklist of domains where the blacklist contains domains that serveads. The domains matched in the blacklist returns a non-existent IP address that results in ads not being fetched and inturn not displayed. Other domains are either resolved by the inbuilt DNS within Adguardor are forwarded to a configured upstream DNS server.

The request is resolved and the website is displayed free of advertisements. The system blocks Ads from being resolvedwhich in-turn prevents tracking and unnecessary network usage.

V. CONCLUSION

This research outcome shows the impact of web browsing activities. The active traffic consumed the highest inbound bandwidth usage in enterprise network environment. With the number of daily online activity of user in enterprise network, online advertising contents might impact high data demand from web browsing activity. As prediction by 2018, 80% of web contents are delivered in media platform [5]. This study has identified current web browsing trends traffic in enterprise network where it consumed around50 percent in average. This statistic is claimed from a study conducted by Malaysian Communications and Multimedia Commission (MCMC) stated that the trends for years 2017, 87% of their respondents used web browser to retrieve information and 67 percent used for formal and informal for study.

This study agrees that both AdBlock techniques perform a reduction of traffic and bandwidth usage. However, the best solution in enterprise network for AdBlocking technique is DNS AdBlock. By implementing DNS AdBlock in enterprise network environment can sustain the usage of web browsing activityfor enterprise network and also it has the potential to generate substantial saving across several fonts. Besides, the implementation of browser extension AdBlock proved that the process of displaying online advertisement drains a significant amount of energy usage. Therefore, when scaled to large network, DNS AdBlock is an effective solution to control of end devices for process of blocking online advertisement.

There are some limitations to Adguard. One of the most important limitations is Ads that have the same domain as the legit traffic won’t be blocked and hence the users are stuck with YouTube Ads even on AdGuard. However that can be improved by generating blacklists that are related to Ads on that domain. Furthermore, parental controls can be added so that parents can block certain devices in the network from accessing adult domains. Another point of recommendation is to allow the user to updateblacklists and reboot the system from theweb panel itself instead of using the console.

REFERENCES

1. Giorgio Brajnik and Silvia Gabrielli. 2010. A review of online advertising effects on the user experience.
2. International Journalof Human-Computer Interaction 26, 10 (2010), 971–997
3. Chang-Hoan Cho and Hongsik John Cheon. 2004. Why do people avoid advertising on the internet? Journal of Advertising 33,4 (2004), 89–97.
4. Steven M Edwards, Hairong Li, and Joo-Hyun Lee. 2002. Forced exposure and psychological reactance: Antecedents and consequences of the perceived intrusiveness of pop-up Ads. Journal of Advertising 31, 3 (2002), 83–95.
5. Avi Goldfarb and Catherine Tucker. 2011. Online display advertising: Targeting and obtrusiveness. Marketing Science 30, 3 (2011), 389–404
6. Wen Li and Ziying Huang. 2016. The Research of Influence Factors of Online Behavioral Advertising Avoidance. American Journal of Industrial and Business Management 6, 09 (2016), 947.
7. Catherine E. Tucker. 2014. Social Networks, Personalized Advertising, and Privacy Controls. Journal of Marketing Research 51, 5 (2014), 546–562.
8. Kiran Garimella, Orestis Kostakis, and Michael Mathioudakis. 2017. Ad-blocking: A Study on Performance, Privacy and Counter-measures. In Proceedings of the 2017 ACM on Web Science Conference (WebSci ’17). ACM, New York, NY, USA,259–262

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details