International Journal of
Technology and Systems
(IJTS)

SECURITY AND NUISANCES OF SOCIAL MEDIA ON WI-FI NETWORK

Fuseini Inusah

IPRJB
INTERNATIONAL PEER REVIEWED
JOURNAL AND BOOK PUBLISHING

Security and Nuisances of Social Media on Wi-Fi Network

[1*]Fuseini Inusah
Student (Phd Computer Science), Department Of Computer Science, Kwame Nkrumah University of Science and Technology

Article History

Received 15th February 2023

Received in Revised Form 25th February 2023

Accepted 8th March 2023

Crossref

Abstract

Purpose: This research is about the nuisances of social media application on a Wi-Fi network in a university campus in Ghana. The aim was to access the security risk on the network, the speed of the network and the data consumption of those platforms on the network. Nmap Zenmap GUI 7.80 application was used to scan the various social media platforms to identify the protocols, ports, services etc. to enable in accessing the vulnerability of the network. Data consumption on users' mobile devices was collected and analyzed.

Methodology: An online questionnaire was also used to solicit for the information on social media data usage from the users of the network.

Findings: The top ten social media platforms i.e. Facebook, WhatsApp, Twitter, YouTube, Messenger, Instagram, Telegram, LinkedIn, Telegram and Tik-Tok are not running on secured protocols and services. This calls for serious attention on the security of networks that allows such application. A proper filtering mechanism is necessary to protect the network from attacks.

Unique Contribution to Theory, Practice and Policy: Entertainment is relevant for education but not mandatory for learning. If social media platforms are posing security threats, increasing unnecessary traffic and resulting to high cost of maintaining networks. The nuisance of social media is as a result of the nature of the content or media that is allowed. Users of a network are often attracted to these content. The ability of the content to lure the users makes it necessary for traffic to be generated on the network through the social media applications.

Keywords: *Data Consumption; Device Accounting; Mobile Devices; Social Media; Wifi Network; Rockus Outdoor AP*

INTRODUCTION

Security of networks as well as data consumption with reference to the traffic on the network are serious issues experts consider in determining the efficiency of a network. The vulnerability of a network as well as the throughput of a network affects the use of the network. College networks are in place to assist in blended learning where traditional classroom learning and online learning can be used to achieve the goal of education to achieve the core mandate of the college. Whereas some colleges choose to run their own e-learning platforms and blend content for their learners, others allow their learners to search for content on different websites to gather their own information. The use of social media platforms is very common in the later. These platforms usually do not have restrictions on the content and protocol in use. Many of the social media platforms use TCP as a major protocol and also run services such as HTTP and HTTPs as major services. These services and protocols however do not guarantee security on a network. The services, protocol and content used on these platforms leads to higher consumption of internet data and bandwidth which eventually introduces traffic and reduces the throughput of the network. This finally affects the college in terms of cost and maintenance of the network.

Nmap Zenmap GUI application was used to scan the network to find out the vulnerabilities with reference to the social media platforms that are allowed on the network and the protocols or services used by the various social media platforms. Top ten (10) social media platforms identified on the network are; Facebook, YouTube, WhatsApp, Messenger, Instagram, Tik-Tok, twitter, LinkedIn, telegram and skype. These platforms were accessed based on Monthly Active Unique Users (MAUU) Monthly Data Usage (MDU) and Monthly Billing Cycle (MBC). The protocols, services and the type of content used on these platforms were also considered. All these were done on the college Wi-Fi network. Device Accounting (DA) data recording was used.

Kwame Nkrumah University of Science and Technology (KNUST) is the second largest university in Ghana located in Kumasi the regional Capital of the second most developed region in the country. It has a student population of 55,590 comprising of 21,285 Undergraduates and 2,306 Postgraduates for the 2019/2020 academic year. The university blends online learning with traditional classroom learning at all levels. The use of Internet is therefore a compulsion but not a choice. Ruckus outdoor AP Wi-Fi network is available in the university campus to enable students and lecturers access the internet at all time. This has a throughput capacities of 800Mbps (2.4GHz) and 1733 Mbps (5GHz). The free access to the internet gives many students the chance to access content on social media platforms with passion. This however does not encourage maximum efficiency on the network since it generates more traffic, introduces latency, pose security threats on the network and also increase the cost of internet data in the university.

According to (Manca *et al*., 2017), the geographical location of a person influences communication. Urban planners should therefore use social media platforms to identify the needs of urban areas in planning. The paper (Arnaboldi *et al*., 2017) reveals that the users of the network visit social media platforms with passion. They demonstrate their ego in sharing content and receiving content with other users. According to (Raptis, 2020) whereas social gatherings are limited by resources, social media interactions are unlimited with more resources which makes users stay longer on it. A careful scan of the network using Nmap Zenmap GUI application revealed some social media platforms as the most visited and frequently access by students. A check on the data usage on the devices also revealed that these applications or platforms are ranked higher in data consumption. This calls for an investigation into the efficiency of the network with reference to the use of these social media platforms.

A mobile and communication technologist (Osseiran *et al*., 2013) categories cost, resources and energy under efficiency in talking about the important fields of future mobile and wireless communication technology. The research also indicated that, the projected traffic exponential increase, emergence of huge amounts of communicating devices and the consistently varied requirements and use cases have to be taken into consideration in the production of future mobile and wireless communication systems.

Checking on the protocols used by the social media platforms, it reveals TCP as the most used protocol by social media platform. HTTP, HTTPs, xmp-client and some unknown services. These pose serious security threats to the network.

LITERATURE REVIEW

Top Social Media Platforms

According to (Lua, 2018) there are top twenty one (21) social medial platforms that can be seen on most websites and for that matter very useful for businesses to market their products. They are used to take full advantage of brand reach, identify and reach out to the right users and also reach social media goals. This makes it important for most of these social media content to be available on many networks thereby making it a nuisance in terms of enhancing the efficiency of the network. However, the social medial platforms mentioned in his research are not necessarily the top ten social media platforms used in the college in terms of the way he ranked them. His ranking was global but this research is limited to only the college.

Protocols Used in Social Media Communications

Protocol refers to a standard set of rules that allows connections between and among devices to exchange information. It determines the type of data, commands and confirmation of data transfer within and across a network. (Barakabitze *et al*., 2020) indicated that, the rise in consumption of multimedia content and the need for high quality content from content providers influences how networks are managed in terms of content segregation. Social media uses multimedia content such as text, graphics, animations, videos and sound. These media elements are often hyperlinked or hypermedia. This is done over the internet with multiple users with TCP as the most used protocol in transmitting the information across networks. According to (Venkatesh et al., 2007) research into TCP performance over Optical Burst Switching (OBS) networks has been a fundamental problem lately.

As a result of congestion control mechanism of TCP and the in-built burst losses in the Optical Burst Switching (OBS) network, the throughput of TCP reduces. This protocol however is a major protocol for every social media platform. Protocols used in these social media platforms are Transmission Control Protocol (TCP), Simple Mail Transfer Protocol (SMTP), and Voice over Internet Protocol (VoIP), User Datagram Protocol (UDP) etc. HyperText Transfer Protocol (HTTP), HyperText Transfer Protocols secured (HTTPs), xmp-client are common services running on the social media platforms. These services are prone to security threats as they are running on open ports especially when used with Transmission Control Protocol (TCP).

According to (Charbonneau & Vokkarane, 2011) TCP-over-OBS can be used as transport standard to support next-generation Internet. Load-balanced routing is known to be improving loss performance over OBS. However, implementing TCP over load-balanced OBS can result to increased out-of-order delivery of TCP packets, which may lead to frequent timeouts and quicker retransmissions. Reordering-Robust TCP (RR-TCP) over OBS networks was realized in performance. It was observed that, standard TCP experiences significant throughput degradation due to persistent packet reordering. It is however worthy to note that all the above interventions will increase the load on a network, increase the delay in packet transmission and also make the network overloaded in terms of software.

Secure Verse Unsecure Protocols

According to (Jang-Jaccard & Nepal, 2014) the unexpected growth in the Internet has increased cyber-attack incidents with more damaging effects. This calls for the use of protocols that can help enhance maximum security. (Osseiran *et al*., 2013) predicted that in 2020, the traffic generated by mobile and wireless devices will increase a thousand times over 2010 figures and also rise in the number of wireless devices connected in tens of billions which will have a deep effect on society. This does not only call for security but the need to boast speed as traffic on networks will increase.

According to (Evans *et a*l., 2016), the choice of a suitable routing protocol for implementation is an important part of every network design. Several decisions are considered in order to select the best protocol for deployment. These decisions include speed, accuracy, security, cost and management of the protocol with reference to the content. This decision in choosing a protocol is necessary in order to protect the network. There is however a challenge in achieving both security and speed at the same time. In (Leira *et al*., 2018), it is indicated clearly that controlling latency is a major concern in SAN. Packet engines such as DPDK, can be used to measure latencies in high-speed optical networks. In the book chapter (Goda, 2016) TCP as a widely used protocol is known for its unsecure ports. Except port 860 and 3260, all other ports on TCP are not secure. A software-based solution to measure latency is better among proposed solutions. An extension that serves to measure bandwidth will also be a good recommendation. However, it is clear that as security is enhanced by introducing software to manage the network, latency is introduced and traffic increased with low throughput.

Network Traffic

This is the amount of data moving across a network at a given point in time. (Shimonski, 2013) opined that If communication device is receiving too much traffic, the device's ability to process the traffic may be jeopardized as it will be overwhelmed. This can cause dropped packets on the network. It is mostly used in Denial of Service (DoS) attacks on networks. The latency introduced by traffic in networks is a major nuisance that drastically reduces the efficiency of the network. This nuisance must be managed in networks. In the paper (Rostami-Shahrbabaki et al., 2020) traffic is seen as a nuisance on the road in urban areas. The conscious effort made to reduce the traffic in that research is assuming availability of connected vehicles data. Two layers i.e link layer and network layer are used to estimate high resolution in seconds for the whole network. This nuisance and the solution applied to it is not completely different from the traffic generated in the Internet. In (Masud *et al.*, 2017), a traffic adaption mechanism is used to manage a wirelessly body area network by adapting Medium Access Control Protocol(MAC) for patients healthcare. This is to enable efficiency by increasing speed, accuracy and easy to work in the health sector. The paper (Tian, 2020) did a network traffic prediction by using chaotic characteristics of network traffic time series collected at different time scales. This was compared to the autocorrelation of network traffic. It was revealed that, network traffic is chaotic. This clear indication of traffic as a nuisance is enough evidence to eliminate traffic on networks.

Carrier Data Accounting (CDA) vrs Device Accounting (DA)

A researcher (Raggo, 2016a) suggested that in developing mobile applications, both security and users of the device should be taken into consideration. The ability of users to access and know the amount of data consumed by them with reference to the applications and the devices they are using is a convenience in the use of smartphones and other mobile devices. According to (Raggo, 2016b) there is a shift from the first generation of mobile devices to more sophisticated and convenient mobile devices for user consumption. These devices are internet enabled devices that use internet data.

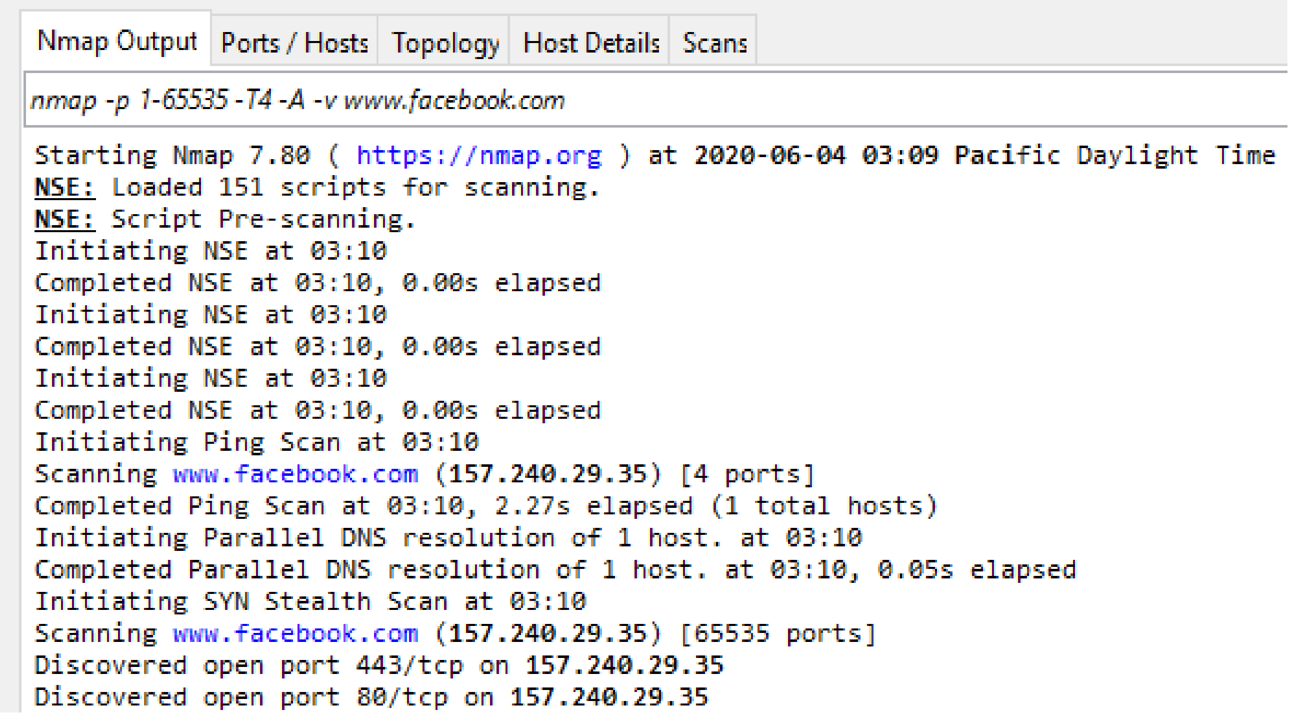
Data consumption on a device may vary from one device to another. As opined in (Cuadra-sánchez, 2016), devices on the network of an organization does consume data to enable in connection to the organization’s network. The calculation of the user on how much data is spent on accessing the internet may differ from the recordings of the device. The former is the carrier data accounting whiles the latter is the device accounting. The variance however should not be so huge. Carrier data accounting is necessary for the user to know the expenditure in using the internet. The calculations of the device on how much data is spent on each application on the internet helps in knowing the applications and the intensity of the application on data consumption. In this research, the device accounting was used to determine how much data the device consumes on the top ten social media network applications. This was necessary to help in knowing the cost involved in managing the network in the university. It was also to help in determining the bandwidth and the congestion as well as traffic on the network.

METHODOLOGY

The research employed experimentation and online questionnaire to collect data. The Nmap Zenmap GUI application was used to scan the various social media platform websites to identify the protocols, ports and services running. It was also to disclose the state of the ports as either close or open to determine level of security. An online questionnaire was also used to solicit for the information on social media data usage from the users of the network. This questionnaire was sent to WhatsApp platforms for the students to provide information on their data consumption. In all, the ten most used social media platforms websites were scanned and about hundred well answered questionnaires were used in the analysis. Averages were used in the analysis of the data.

Procedure in Data Collection

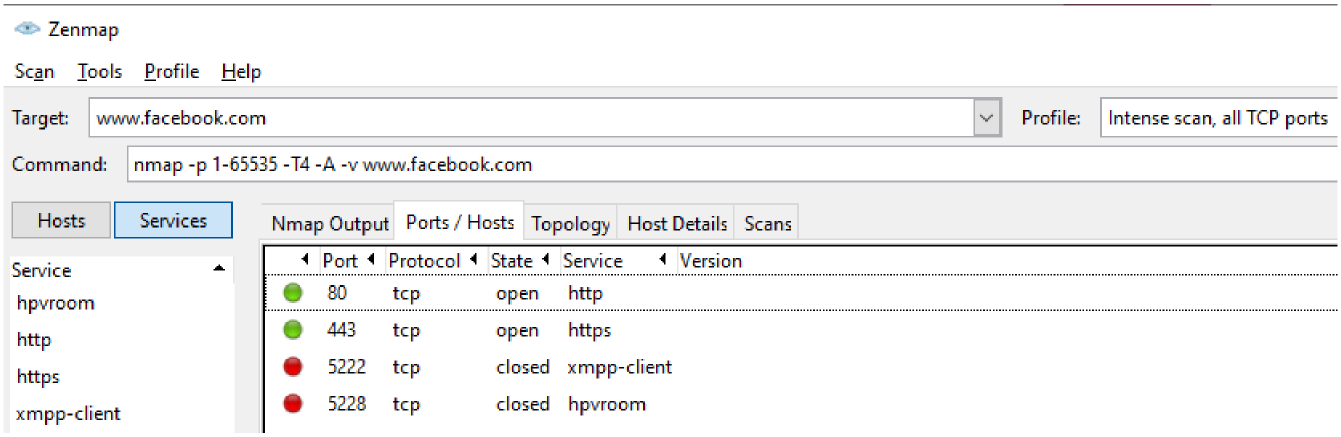
Each of the top ten social media platform was scanned using the Nmap Zenmap 7.80 application. It was an intense scan on all TCP ports. This was done to identify the protocol, port, state of the port (open or close) and services running. It was necessary to know the strengths and weaknesses of the websites visited in terms of security. Figure 1shows scan results of Facebook with reference to the protocol, ports and services running.



```
nmap -p 1-65535 -T4 -A -v www.facebook.com
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-04 03:09 Pacific Daylight Time
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:10
Completed NSE at 03:10, 0.00s elapsed
Initiating NSE at 03:10
Completed NSE at 03:10, 0.00s elapsed
Initiating NSE at 03:10
Completed NSE at 03:10, 0.00s elapsed
Initiating Ping Scan at 03:10
Scanning www.facebook.com (157.240.29.35) [4 ports]
Completed Ping Scan at 03:10, 2.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:10
Completed Parallel DNS resolution of 1 host. at 03:10, 0.05s elapsed
Initiating SYN Stealth Scan at 03:10
Scanning www.facebook.com (157.240.29.35) [65535 ports]
Discovered open port 443/tcp on 157.240.29.35
Discovered open port 80/tcp on 157.240.29.35
```

```
PORT     STATE      SERVICE    VERSION
80/tcp   open       http
443/tcp  open       ssl/https
5222/tcp closed     xmpp-client
5228/tcp closed      hpvroom
```



Target: www.facebook.com
Profile: Intense scan, all TCP ports
Command: nmap -p 1-65535 -T4 -A -v www.facebook.com

Service
hpvroom
http
https
xmpp-client

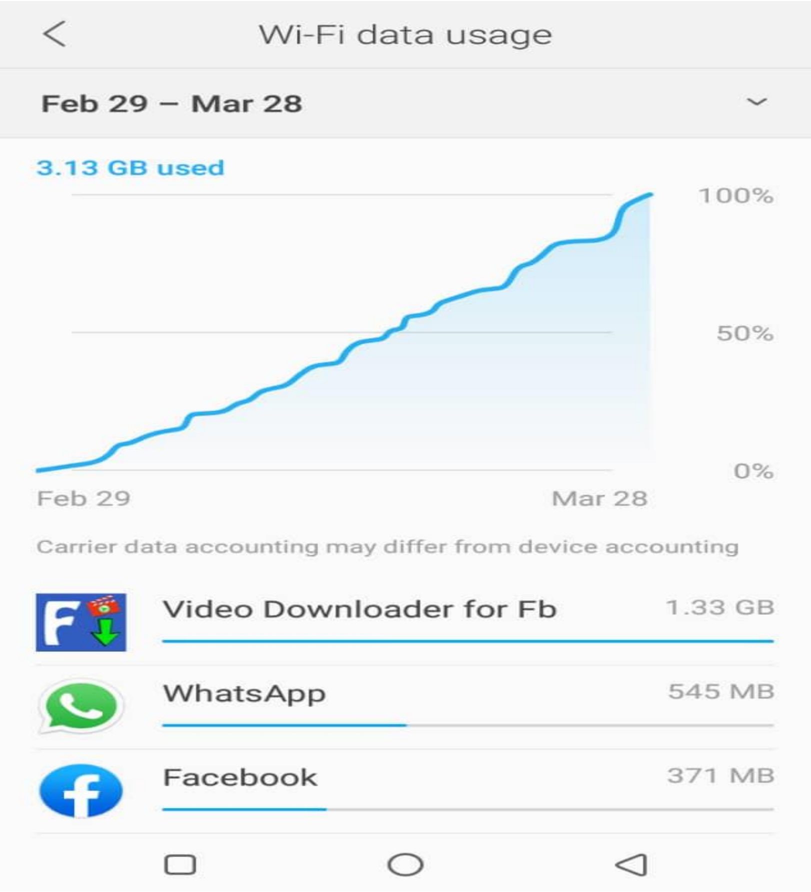
Port	Protocol	State	Service	Version
🟢 80	tcp	open	http	
🟢 443	tcp	open	https	
🔴 5222	tcp	closed	xmpp-client	
🔴 5228	tcp	closed	hpvroom	

Figure 1: Facebook Scan Results

The questionnaire used to collect data from users of the network (students and lecturers) was organized in terms of the data consumption rate for each user. This was done by collecting information on mobile devices such as smartphone and laptops. The default billing cycle for the devices is monthly of 30 days. The step below was followed to record information on smart phones.

1. Go to Settings
2. Data usage
3. Wi-Fi data usage
4. Tap on the date on top right Conner of graph
5. Select each most previous duration consumption and record each application's data consumption.

This procedure was used just to know the device data accounting for the social medial applications looked at. It is worth noting that device accounting may be different from carrier data accounting.



Carrier data accounting may differ from device accounting

Video Downloader for Fb	1.33 GB
WhatsApp	545 MB
Facebook	371 MB

Figure 2: Interface of the Wi-Fi Data Usage

FINDINGS

Nmap Scan Results

The results of the Nmap Zenmap application was analyzed and organized in a tabular form for easy understanding. It was seen that all the social media applications are running on TCP as a protocol, have http as service for the application and at least one open port. This pose a serious security threat on the network. Table 1 shows the results

Table 1: Nmap Scan Results

HOST NAME	PORT	State	SERVICES	PROTOCOL
Facebook	80	Open	http	TCP
	443	Open	https	
	5222	Closed	xmpp-client	
	843	Closed	applications	
WhatsApp	80	Open	http	TCP
	443	Open	https	
	5222	Closed	xmpp-client	
	843	Closed	Applications	
Twitter	80	Open	http	TCP
	443	Open	https	
Messenger	80	Open	http	TCP
	443	Open	https	
	5222	Closed	xmpp-client	
	843	Closed	applications	
YouTube	80	Open	http	TCP
	443	Open	https	
Instagram	80	Open	http	TCP
	443	Open	https	
	5222	Closed	xmpp-client	
	843	Closed	Applications	
Tik-Tok	80	Open	http	TCP
	443	Open	https	
	53	Closed	Domain	
LinkedIn	443	Open	https	TCP
	53	Closed	Domain	
Telegram	80	Open	http	TCP
	443	Open	https	
	53	Closed	Domain	
Skype	80	Open	HTTP	TCP, UDP

All the social media platforms use TCP which does not protect a segment against message change attacks. TCP does not protect networks against the illegal access attacks. It has a field used in order to recognize a change of a segment. However, since this field is not protected against the message modification attacks, it is possible to modify any TCP segments because it cannot keep segment data secure against the message eavesdropping attacks. TCP transports data in the application layer but since it does not provide any data encryption functions, anyone can gain access to any valuable information. TCP verifies a peer device by using the source IP address and a port number. However, it is possible to modify the source address and port number. Since all the social media platforms has one or more ports opened, it pose very serious security threats since an attacker can attack the network through this. All social media platforms are running on Http and https which is an open port and allowing traffic outbound on networks. All social media platforms use http services which is not secure.

Data Consumption

The data consumption on the social media applications were recorded and analyzed. Three previous months data consumption was recorded to know the pattern of consumption. RapidMiner Studio Educational 9.6.00 was used to validate the data from users to eliminate incomplete data to enhance more accuracy in analysis. After validation, 100 participants accurately produced the data. The refined data was then copied to Microsoft excel to analyze. This was done in separate sheets in Microsoft excel for analysis. Each month's data consumption was analyzed in terms of the minimum consumption, maximum consumption, averages and the total data consumptions on all the ten social media platforms by a user. This was necessary to know the rate at which users of the network used the data on the social medial platforms and also determine the average, minimum, maximum and MAUU cost of data for the university.

For the first month, Facebook recorded an average of 621.78MB, minimum of 198MB, maximum of 948MB and MAUU of 53 users. WhatsApp recorded average of 604.33MB, minimum of 402MB, maximum of 855MB and MAUU of 51 users. Twitter recorded an average of 267.39MB, minimum of 103MB, maximum of 491MB and MAUU of 48 users. YouTube recorded an average of 689.86MB, minimum of 500MB and maximum of 896MB with MAUU of 48 users. Messenger recorded an average of 175.4 MB, a minimum of 105MB maximum of 312MB and MAUU of 38 users. Instagram recorded an average of 502.51MB, minimum of 236MB, maximum of 745MB and MAUU of 62 users. Telegram recorded average of 200.72MB, minimum of 105MB, maximum of 456MB and MAUU of 48 users. Skype recorded an average 465.5MB, minimum of 109MB, maximum of 928MB and MAUU of 55 users. Tik-Tok recorded an average 512.5MB, minimum of 245MB, Maximum of 875MB and MAUU of 50 users. And LinkedIn recorded an average of 238.76MB, minimum of 107MB, maximum of 498MB and MAUU of 45 users. The overall average consumption for all platforms is about 4278.82MB with minimum consumption per user as 3467MB, maximum consumption per user as 5522MB.

In the second month, Facebook recorded an average of 630.4MB, minimum of 245MB, maximum of 890MB, and MAUU of 55 users. WhatsApp recorded an average of 607.78MB, minimum of 221MB, maximum of 928MB and MAUU of 45 users. Twitter recorded 395MB, minimum of 105MB, maximum of 745MB and MAUU of 56 users. YouTube recorded an average of 658.22MB, a minimum of 402MB, maximum of 948MB and MAUU of 49 users. Messenger recorded an average of 233.89MB, minimum of 105MB, maximum of 513MB and MAUU of 45 users. Instagram recorded an average of 346.92MB, minimum of 103MB, maximum of 745MB and MAUU of 45 users. Telegram recorded 195.75MB, minimum of 105MB, maximum of 312 and MAUU of 53 users. Skype recorded an average of 532.78MB, minimum of 299MB, maximum of 811MB and MAUU of 41 users. Tik-Tok recorded an average of 554.32MB, minimum of

247MB, Maximum of 875MB and MAUU of 45 users. And LinkedIn recorded an average of 186.88MB, minimum of 105MB, maximum of 350MB and MAUU of 43 users.

For the third month, Facebook recorded an average of 495.51MB, minimum of 109MB, maximum of 928MB and MAUU of 56 users. WhatsApp recorded an average of 622.83MB, minimum of 259MB, maximum of 892MB and MAUU of 52 users. Twitter recorded an average of 241MB, minimum of 105MB, maximum of 491MB and MAUU of 46 users. YouTube recorded average of 657.43MB, minimum of 254MB, maximum of 948MB and MAUU of 46 users. Messenger recorded an average of 197.44MB, minimum of 103MB, maximum of 441MB and MAUU of 41 users. Instagram recorded an average of 534.71MB, minimum of 236MB, maximum of 856MB and MAUU of 48 users. Telegram recorded an average of 204.1MB, minimum of 105MB, maximum of 452MB and MAUU of 50 users. Skype recorded an average of 477.3MB, minimum of 165MB, maximum of 875MB and MAUU of 56 users. Tik-Tok recorded an average of 597MB, minimum of 253MB, maximum of 874MB and MAUU of 49 users. And LinkedIn recorded an average of 243.5MB, minimum of 108MB, maximum of 498MB and MAUU of 48 users. The overall average consumption was 4267.69MB with a minimum of 3468MB, maximum of 5185MB and MAUU of 47 users. Figure 2, figure 3 and figure 4 are graphs representing the recordings for the first, second and third month respectively. The averages were compared in a line graph to know the true pattern of data consumption. This can be seen in figure 5. Table 2 shows data on three months minimum, average and maximum consumption.

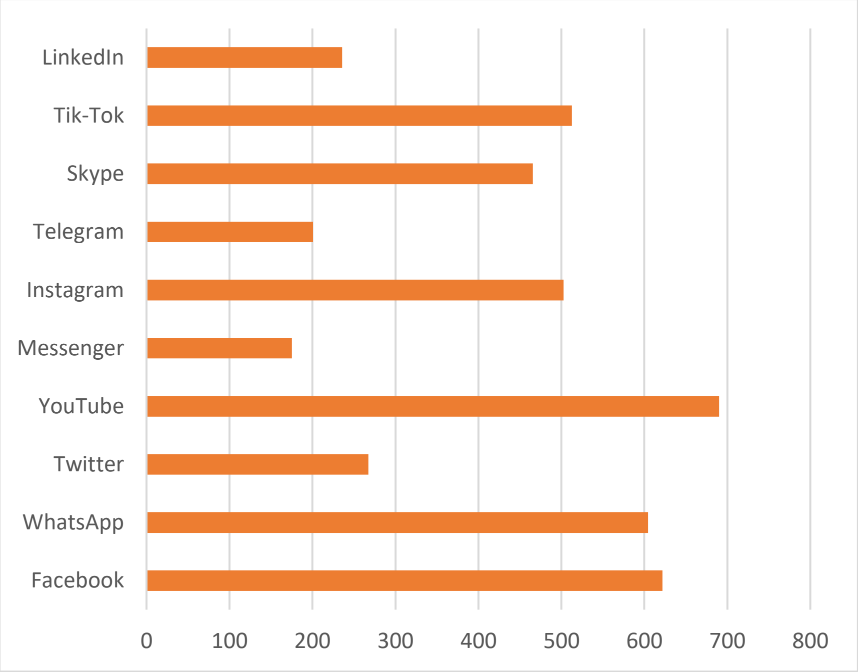


Figure 3: First Month’s Average Data Consumption on Social Media Applications

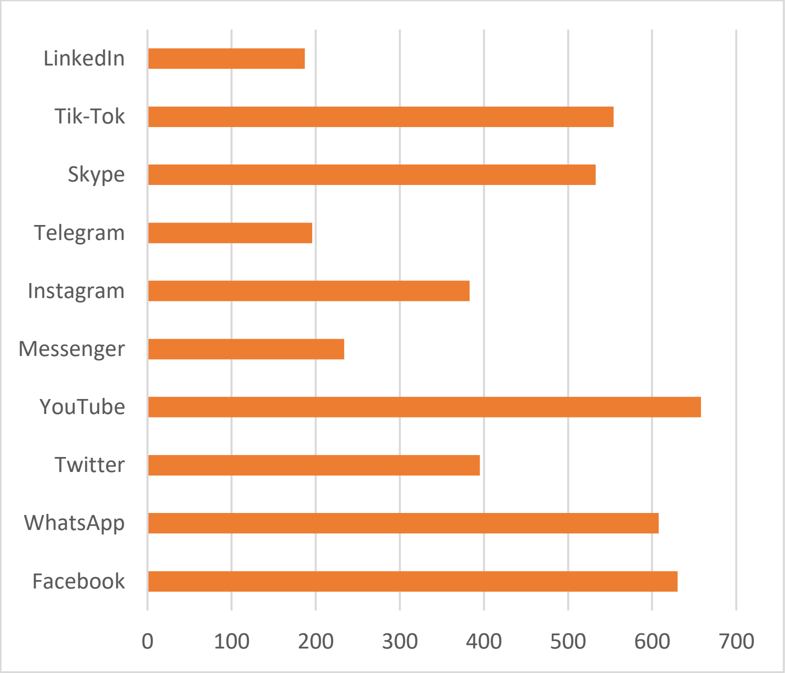


Figure 4: Second Month's Averages on Data Consumption

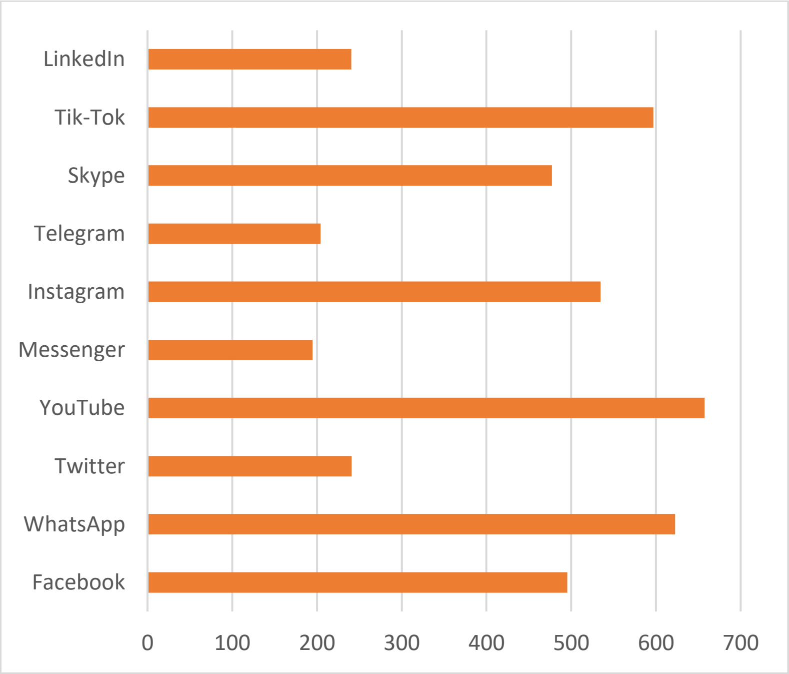


Figure 5: Third Month's Averages on Data Consumption

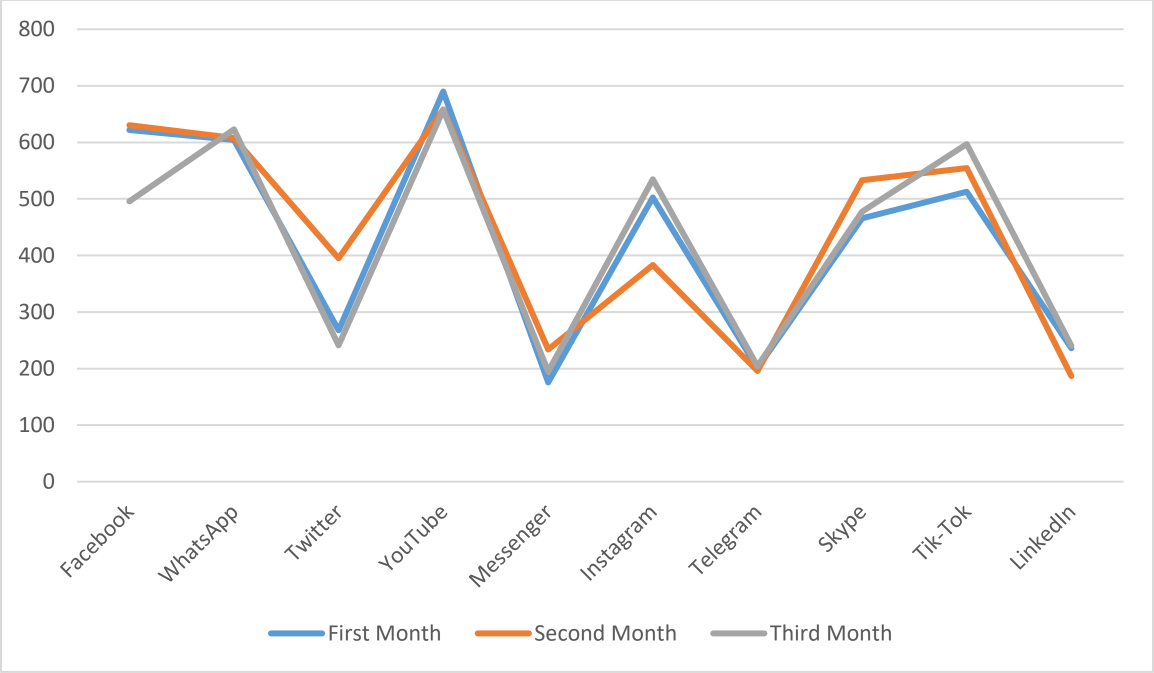


Figure 6: Line Graph Comparing the Averages of the Three Months

Table 2: Comparing Three Months Data Consumption Analysis

Application	Data consumption								
	First month			Second Month			Third Month		
	Min	Average	Max	Min	Average	Max	Min	Average	Max
Facebook	198	621.78	948	245	630.4	890	109	495.51	928
WhatsApp	402	604.33	855	221	607.78	928	259	622.82	892
Twitter	103	267.39	491	105	395	745	105	241	491
YouTube	500	689.89	896	402	658.22	948	254	657.43	948
Messenger	105	175.4	312	105	233.89	513	103	194.77	441
Instagram	236	502.51	745	103	346.92	745	236	534.71	856
Telegram	105	200.72	456	105	195.75	312	105	204.1	452
Skype	109	465.5	928	299	532.78	811	165	477.3	875
Tik-Tok	245	512.5	875	247	554.32	875	253	597	874
LinkedIn	107	238.76	498	105	186.88	350	108	243.5	498

Summary

The top ten social media platforms i.e. Facebook, WhatsApp, Twitter, YouTube, Messenger, Instagram, Telegram, LinkedIn, Telegram and Tik-Tok are not running on secured protocols and services. This calls for serious attention on the security of networks that allows such application. A proper filtering mechanism is necessary to protect the network from attacks.

With an individual average user data consumption of 4278.82MB in first month, 4341.97MB in second month and 4267.49MB in third month, it is clear that an individual user of the network consumes not less than 4296MB. This is equivalent to 4 gigabytes, 300 megabytes. This rate at which youngsters especially students connect to social media platform with passion gives a clear indication that cost of data and traffic on networks will be a challenge if these social media applications are allowed to run. It is therefore necessary for network administrators to control these social media platforms and limit the activities on it to reduce the traffic generated on the network and allow more important content to gain priority. For maximum efficiency, educational institutions should adopt “zero data” for e-learning platforms and reduce data availability for free browsing on social media websites in other to make learners frequently access educational materials and reduce the cost of managing the networks. A URL Filtering on the Rockus Outdoor Ap will also be effective for solving the problem

CONCLUSION AND RECOMMENDATIONS

Entertainment is relevant for education but not mandatory for learning. If social media platforms are posing security threats, increasing unnecessary traffic and resulting to high cost of maintaining networks, then it is necessary to filter the social media applications to pave way for more educational content in the university’s network. The nuisance of social media is as a result of the nature of the content or media that is allowed. Users of a network are often attracted to these content. The ability of the content to lure the users makes it necessary for traffic to be generated on the network through the social media applications. As the users of the network are students at both undergraduate and post graduate levels, the use of the social media platforms cannot be minimized on the network if the media is allowed to run. The only reliable way of doing away with the nuisance is by filtering the social media applications to give educational content more priority on the network. This will reduce the time users of the network spend on the social media applications and also increase the time used on educational content.

The security of the network will be boasted if the social media applications are not allowed to run on the network. It is clear that the protocols as well as the ports and services running on the social media applications are not secured. This pose a lot of security threats on the network. This can result to serious attacks on the network and loss of vital information. Filtering these social media applications from the network is therefore a necessity.

On the issue of the traffic generated by the social media platforms, the nature of the users of the network makes it difficult to have the media running on the network and also achieving high bandwidth and throughput for the network. Majority of the traffic generated on the network is social media content related and the passion in accessing the content is as a result of the luring nature of the content. Filtering this platforms will therefore allow better content to be available and used on the network.

Cost of maintenance on the network is higher as a result of the data consumed and the security updates and or patches needed in handling the vulnerabilities on the network. The college spends so much in providing data for the network due to the rate at which data is being consumed on the social media platforms at the expense of the educational content and other relevant content. The most effective way of managing this expenditure is to minimize or eliminate the social media platform or content on the network. This can be done through filtering of the social media platforms to allow relevant academic content to gain priority on the network. A URL filtering of the social media websites will be more efficient in handling this problem.

REFERENCES

Arnaboldi, V., Conti, M., Passarella, A., & Dunbar, R. I. M. (2017). Online Social Networks and information diffusion: The role of ego networks. *Online Social Networks and Media*, *1*, 44–55. https://doi.org/10.1016/j.osnem.2017.04.001

Barakabitze, A. A., Ahmad, A., Mijumbi, R., & Hines, A. (2020). 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*, *167*. https://doi.org/10.1016/j.comnet.2019.106984

Charbonneau, N., & Vokkarane, V. M. (2011). Performance modeling of HS-RR-TCP over load-balanced optical burst-switched (OBS) networks. *Optical Switching and Networking*, *8*(2), 116–128. https://doi.org/10.1016/j.osn.2010.10.002

Cuadra-sánchez, A. (2016). Mobile Data Loss: Threats and Countermeasures. *Network Security*, *2016*(6), 4. https://doi.org/10.1016/s1353-4858(16)30054-x

Evans, G., Asante, M., & Acheampong Amponsah, A. (2016). Dynamic Routing Implementation Decision between OSPFv3 and IS–IS in IPv6 Networks. *Communications on Applied Electronics*, *6*(3), 25–34. https://doi.org/10.5120/cae2016652446

Goda, K. (2016). Storage Area Network. *Encyclopedia of Database Systems*, 1–2. https://doi.org/10.1007/978-1-4899-7993-3_1329-2

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Leira, R., Aracil, J., López de Vergara, J. E., Roquero, P., & González, I. (2018). High-speed optical networks latency measurements in the microsecond timescale with software-based traffic injection. *Optical Switching and Networking*, *29*(March), 39–45. https://doi.org/10.1016/j.osn.2018.03.004

Manca, M., Boratto, L., Morell Roman, V., Martori i Gallissà, O., & Kaltenbrunner, A. (2017). Using social media to characterize urban mobility patterns: State-of-the-art survey and case-study. *Online Social Networks and Media*, *1*, 56–69. https://doi.org/10.1016/j.osnem.2017.04.002

Masud, F., Abdullah, A. H., Abdul-Salaam, G., & Ullah, F. (2017). Traffic adaptive MAC protocols in wireless body area networks. *Wireless Communications and Mobile Computing*, *2017*. https://doi.org/10.1155/2017/8267162

Osseiran, A., Braun, V., & Hidekazu, T. (2013). The foundation of the mobile and wireless communications system for 2020 and beyond. *Proc. IEEE Veh. Tech. …*, 1–5. https://doi.org/10.1109/VTCSpring.2013.6692781

Raggo, M. T. (2016a). Developing Your Mobile Device Security Strategy. *Mobile Data Loss*, 37–43. https://doi.org/10.1016/b978-0-12-802864-3.00005-2

Raggo, M. T. (2016b). Preparing for Generation Mobile. In *Mobile Data Loss* (pp. 1–6). Elsevier. https://doi.org/10.1016/b978-0-12-802864-3.00001-5

Raptis, T. P. (2020). When Wireless Crowd Charging Meets Online Social Networks: A Vision for Socially Motivated Energy Sharing. *Online Social Networks and Media*, *16*, 100069. https://doi.org/10.1016/j.osnem.2020.100069

Rostami-Shahrbabaki, M., Safavi, A. A., Papageorgiou, M., Setoodeh, P., & Papamichail, I. (2020). State estimation in urban traffic networks: A two-layer approach. *Transportation Research Part C: Emerging Technologies*, *115*, 102616. https://doi.org/10.1016/j.trc.2020.102616

Shimonski, R. (2013). Deep Analysis. *The Wireshark Field Guide*, 101–118. https://doi.org/10.1016/b978-0-12-410413-6.00009-7

Tian, Z. (2020). Chaotic characteristic analysis of network traffic time series at different time scales. *Chaos, Solitons and Fractals*, *130*. https://doi.org/10.1016/j.chaos.2019.109412

Venkatesh, T., Praveen, K., Sujatha, T. L., & Murthy, C. S. R. (2007). Performance evaluation of high speed TCP over optical burst switching networks. *Optical Switching and Networking*, *4*(1), 44–57. https://doi.org/10.1016/j.osn.2006.09.005